NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MOBILE DEVICE MANAGEMENT IN THE DOD ENTERPRISE NETWORK: FACTORS FOR RISK MANAGEMENT, INTEGRATION, AND IT ACQUISITION

by

Donald E. Pratt Jr.
Brian K. Jones

March 2013

Thesis Advisor:	Glenn Cook
Thesis Co-Advisor:	Brad Naegle
Third Reader:	Douglas Brinkley

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704–0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE MOBILE DEVICE MANAGEMENT IN THE DoD ENTERPRISE NETWORK: FACTORS FOR RISK MANAGEMENT, INTEGRATION, AND IT ACQUISITION		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Donald E. Pratt Jr. and Brian K. Jones			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Naval Postgraduate School Acquisition Research Program		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

The Office of the Department of Defense Chief Information Officer (DoD CIO) has developed a mobile device strategy that will require the DoD information technology (IT) system acquisition process to acquire a mobile device management (MDM) toolset to mitigate information assurance (IA) risks created through the use of mobile devices on the enterprise domain. In an effort to target affordability and control cost growth, IT professionals need to understand how IA concerns are addressed through MDM and how properly scoped solutions can be sourced to reduce project risks related to cost, schedule, and performance for projects that involve obtaining an MDM toolset through the DoD acquisition process.

This research develops a mixed method study to understand the concerns of federal information technology professionals who are knowledgeable on MDM and the acquisition professionals who procure the MDM solutions. In this research, the authors provide DoD professionals with a framework to select optimal MDM solutions through the identification of baseline requirements in order to operate effectively in a resource constrained environment.

14. SUBJECT TERMS Mobile Device Management, MDM, Mobile Device Security, Information Assurance, IA, Information Technology Management, ITM, Cost Effectiveness Analysis, CEA, Enterprise Architecture			**15. NUMBER OF PAGES** 187
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MOBILE DEVICE MANAGEMENT IN THE DoD ENTERPRISE NETWORK: FACTORS FOR RISK MANAGEMENT, INTEGRATION, AND IT ACQUISITION

Donald E. Pratt Jr.
Major, United States Army
B.B.A., Texas Christian University, 2003
Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

Brian K. Jones
Major, United State Army
B.S., East Tennessee State University, 2000
Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2013

Authors: Donald E. Pratt Jr.
Brian K. Jones

Approved by: Glenn Cook
Thesis Advisor

Brad Naegle
Thesis Co-Advisor

Douglas Brinkley
Thesis Third Reader

Dan Boger
Chair, Department of Information Sciences

William R. Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Office of the Department of Defense Chief Information Officer (DoD CIO) has developed a mobile device strategy that will require the DoD information technology (IT) system acquisition process to acquire a mobile device management (MDM) toolset to mitigate information assurance (IA) risks created through the use of mobile devices on the enterprise domain. In an effort to target affordability and control cost growth, IT professionals need to understand how IA concerns are addressed through MDM and how properly scoped solutions can be sourced to reduce project risks related to cost, schedule, and performance for projects that involve obtaining an MDM toolset through the DoD acquisition process.

This research develops a mixed method study to understand the concerns of federal information technology professionals who are knowledgeable on MDM and the acquisition professionals who procure the MDM solutions. In this research, the authors provide DoD professionals with a framework to select optimal MDM solutions through the identification of baseline requirements in order to operate effectively in a resource constrained environment.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

APB	Acquisition Program Baseline
BYOD	Bring Your Own Device
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAC/PIV	Common Access Card/Personal Identification Verification
CEA	Cost Effectiveness Analysis
CERDEC	Communication Electronics Research, Development, and Engineering Center
CFO	Chief Financial Officer
CIO	Chief Information Officer
C-level	Corporate Level
CNO	Computer Network Operations
CoN	Certificate of Networthiness
COO	Chief Operations Officer
CSS	Central Security Service
CTE	Critical Technology Element
CTO	Chief Technology Officer
DAA	Designated Approval Authority
DAE	Defense Acquisition Executive
DAWIA	Defense Acquisition Workforce Improvement Act
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DoS	Denial of Service
DRD DDR&E	Director, Research Directorate, Office of the Director, Defense Research and Engineering
EA	Enterprise Architecture
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standard
FIS	Foreign Intelligence Service
FY	Fiscal Year
GAL	Global Address List
GAO	Government Accountability Office
GPS	Global Positioning System

IA	Information Assurance
IAM	Information Assurance Management
IASM	Information Assurance Security Manager
IASO	Information Assurance Security Officer
IC	Intelligence Community
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMEI	International Mobile Station Equipment Identity
IP	Internet Protocol
IR	Infrared
IR	Interagency Report
IRB	Institutional Review Board
IT	Information Technology
ITIM	Information Technology Investment Management
ITM	Information Technology Management
JCIDS	Joint Capabilities Integration System
MANET	Mobile Ad-Hoc Network
MDM	Mobile Device Management
MitM	Man-in-the-Middle
NA	Network Administrator
NASA	National Aeronautics and Space Administration
NFC	Near Field Communications
NIST	National Institute of Standards and Technology
NPRST	Navy Personnel Research, Studies, and Technology
NSA	National Security Agency
NSEC	National Security Engineering Center
ODNI	Office of the Director of National Intelligence
OHRS	Occupational Health Record-Keeping System
OS	Operating System
OTA	Over-the-Air
PM NES	Program Manager Network and Enterprise Services
PQM	Program Quality Management
RDECOM	Research Development and Engineering Command
RFI	Request for Information
ROI	Return on Investment
S/MIME	Secure/Multipurpose Internet Mail Extension

SA	System Administrator
SaaS	Software-as-a-Service
SCEP	Simple Certificate Enrollment Protocol
SIGINT	Signals Intelligence
SME	Subject Matter Expert
SPRDE	System Planning, Research, Development, and Engineering
TCO	Total Cost of Ownership
TRA	Technology Readiness Assessment
TRL	Technology Readiness Level
TTPs	Tactics, Techniques, and Procedures
USB	Universal Serial Bus
VPN	Virtual Private Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to begin by thanking those closest to us: Andy, Auri, Calyx, and Izzy Pratt; and Heidi, Austin, Juliana, and Ian Jones. Our success was only possible through your reassurance, backing, and never-ending patience. We lack the words to convey our gratitude and heartfelt appreciation.

Where could we be without the support, guidance, and encouragement from our advisors: Professor Glenn Cook, Professor Brad Naegle, and Dr. Douglas Brinkley. Thank you for your flexibility and fortitude to see this to the end.

To the Acquisition Research Program, RADM James Greene, USN (Ret), Ms. Karey Shaffer, and Ms. Tera Yoder, your resources and assistance were critical to the realization of our thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

The Office of the Department of Defense Chief Information Officer (DoD CIO) has developed a mobile device strategy that will require the DoD information technology (IT) system acquisition process to acquire a mobile device management (MDM) toolset to mitigate information assurance (IA) risks created through the use of mobile devices on the enterprise domain. However, applications set constraints that impact system hardware and network requirements (Englander, 2009). In an effort to target affordability and control cost growth, IT professionals need to understand how IA concerns are addressed through MDM and how properly scoped solutions can be sourced to reduce project risks related to cost, schedule, and performance for projects that involve obtaining an MDM toolset through the DoD acquisition process. The problem is that acquisition professionals lack the necessary baseline capabilities and technical boundaries, which limits their ability to properly source MDM solutions that will effectively integrate into the DoD enterprise architecture.

B. PURPOSE STATEMENT

The purpose of this research is to develop a mixed method study to understand the concerns of federal information technology professionals who are knowledgeable on MDM and the acquisition professionals who procure the MDM solutions. This research is crucial in support of DoD efforts to secure the network while providing maximum productivity and flexibility to the end user. In this research, the authors provide DoD professionals with a framework to select optimal MDM solutions through the identification of baseline requirements in order to operate effectively in a resource constrained environment.

C. RESEARCH QUESTIONS

- How can the DoD evaluate multiple MDM systems to produce the optimal MDM solution for a given department or organization?

- What is an effective approach for the DoD to identify the most critical evaluation factors when choosing MDM solutions?
- How can the DoD identify critical technology elements (CTE) for MDM?

D. RESEARCH METHODS

A series of questions are drawn from existing research, literature, and personal experience that aim to stratify evaluation criteria and identify CTEs for MDM solutions. The questions focus on DoD MDM implementation, acquisition strategy, and functional capabilities. The final product is a mixed method survey and interview template intended for federal IT and acquisitions professionals with a functional knowledge of MDM.

The survey and interview questions are subdivided into logical categories that allow for the efficient capture of information including the following: the preclusion of unqualified respondents, demographics, the relative importance of capabilities, and any additional comments concerning MDM.

Chapter IV discusses each area of the survey and interview questions in further detail to provide follow-on researchers with a comprehensive understanding of the intended research methodology.

E. DATA, OBSERVATION, AND ANALYSIS METHODS

Based on the survey and interview data, the researchers identified questions that would be the most relevant to DoD IT and acquisition professionals. Some data may not be credible and may require further analysis or exclusion. Suggestions are offered to follow-on researchers regarding the execution of the survey and the use of automated survey tools to aid with the capture, organization, and analysis of raw data.

II. LITERATURE REVIEW

A. DEFINITION OF A MOBILE DEVICE

The National Institute of Standards and Technology (NIST; Scarfone & Souppaya, 2012) defines the baseline of features that make up a mobile device as follows:

- A small form factor;
- At least one wireless network interface for Internet access (data communications) that uses Wi-Fi, cellular networking, or other technologies that connect the mobile device to network infrastructures with Internet connectivity;
- Local built-in (non-removable) data storage;
- An operating system that is not a full-fledged desktop or laptop operating system;
- Applications available through multiple methods (provided with the operating system, accessed through the web browser, acquired and installed from third parties); and
- Built-in features for synchronizing local data with a remote location (desktop or laptop computer, organization servers, telecommunications provider servers, other third party servers, etc.).

B. MOBILE DEVICE USAGE

Mobile device usage is expanding at a rapid pace. A 2011 Cisco Systems' forecast predicts that by 2015, there will be nearly 15 billion network-connected mobile devices, about two for every person on the planet (Burt, 2011). Mobile technology increases the speed at which people acquire and generate data (Boyles, Smith, & Madden, 2012). Technological advances in mobile device processing and storage provide users with capabilities comparable to traditional laptop and desktop computers. The increase of mobile device use and capabilities has also increased their capacity for exploitation, therefore escalating their overall security risk to the enterprise.

C. MOBILE DEVICE THREATS

There are an ever-increasing number of attacks on mobile devices. Malicious software, referred to as malware, on mobile devices increased by 155 percent in 2011, while mobile device security vulnerabilities increased by 93 percent in 2011 (Government Accountability Office [GAO], 2012). Over a 10-month period, from July 2011 to May 2012, mobile malware variants increased from 14,000 to 40,000 (GAO, 2012).

1. Sources of Mobile Threats

These attacks come from several different sources, including botnet operators, cybercriminals, foreign governments, hackers, and terrorists (GAO, 2012; see Appendix A). Botnet operators, also known as "botherders" or "botmasters," are owners of information systems that have been compromised with a malware code that provides access to the information system's resources (Harris, 2010b). The bot herder employs numerous compromised information systems (*bot* is short for robot, including a zombie or drone) resources for various functions, such as the transmission of illicit data or attacks on other information systems (Stalling, Brown, Bauer, & Howard, 2008a). Typically, this is done in a fee-for-service arrangement in which the bot herder utilizes the bots in an attempt to mask the original source of the data or attack (Harris, 2010b). Figure 1 shows a model of an example botnet.

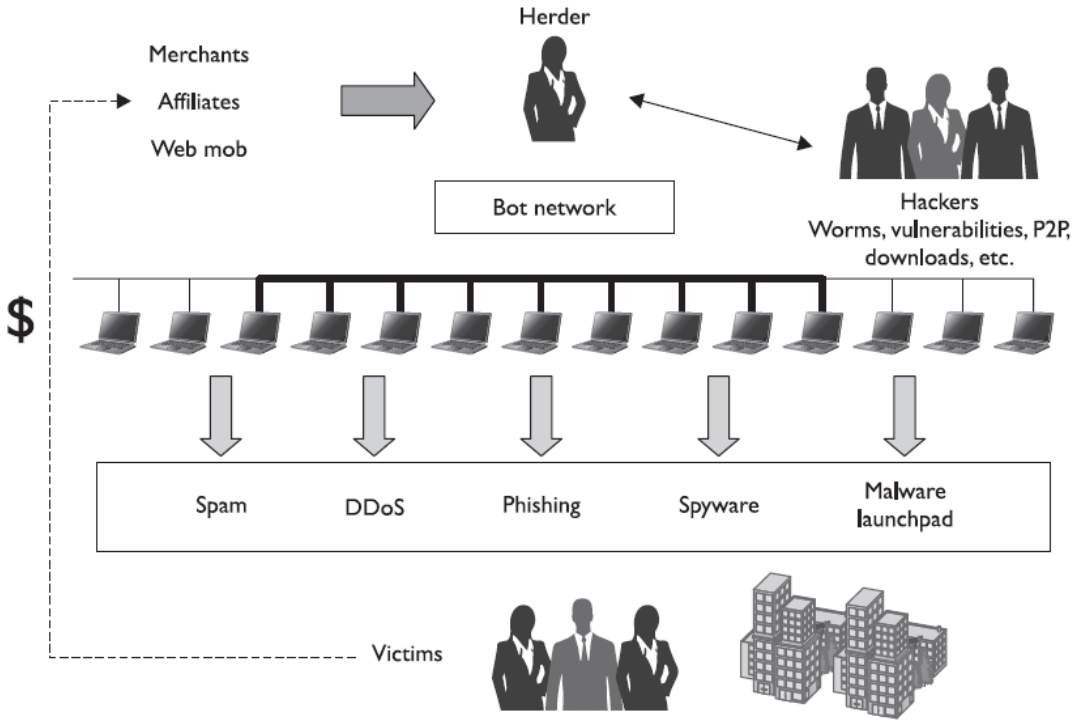


Figure 1. Botnet Diagram (From Harris, 2010b, p. 1021)

Kim Taiple (2012) describes cybercrime as a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity. Financial gain is the motivating force behind cybercriminals. They use illicit attack vectors to obtain data from devices, which is used to commit computer hacking, fraud, and other Internet-related crimes. Industrial espionage, intellectual property, and large-scale monetary theft present viable threats from groups of cybercriminals, not only to corporations and similar institutions but also to government agencies (GAO, 2012).

A foreign intelligence service (FIS) may utilize signals intelligence (SIGINT) against mobile devices in the data-gathering stage (Office of the Director of National Intelligence [ODNI], 2012). Additionally, foreign governments may support the development of material solutions and tactics, techniques, and procedures (TTPs) that could deny or disrupt data (supply, voice, economic) vital to homeland security and

national defense (GAO, 2012). The computer systems of U.S. government agencies and U.S. companies are repeatedly subjected to hacking by about 140 different foreign intelligence organizations, as reported by U.S. counterintelligence (Wilson, 2008).

Tamara Dean (2010) defines a hacker as a person who masters the inner workings of operating systems and utilizes these systems in an effort to better understand them. Walker (2012a) further differentiates the term *hacker* into four classes: black hat, white hat, gray hat, and suicide. Black hats do not apply for authorization or approval to access information systems, but unlawfully use expertise for individual achievement or malevolent intent. White hats apply for authorization or approval to access information systems and use their expertise for refining security or for other protective purposes. Gray hats group individuals who are interested in hacking TTPs and who believe that security flaws in systems should be revealed. Individuals in the final category, suicide hackers, believe that their actions prevail over any prospective penalty. Note that hacking TTPs, which once required a robust base of computer knowledge and skills, can now be utilized by novices, also known as script kiddies, in downloadable form, allowing for ease of use against mobile devices (GAO, 2012).

Terrorists, in an effort to harm national security, stall the U.S. economy, or limit the public trust and confidence, may attempt to ruin, weaken, or take advantage of vital infrastructures such as mobile networks. Attacks vectors, such as phishing schemes or spyware/malware against mobile devices with sensitive information, could be targeted for exploitation (GAO, 2012).

2. Common Mobile Device Attacks

Mobile threat sources can conduct attacks on mobile devices through the exploitation of hardware, software, and users. Common mobile attacks include the following: browser exploits, data interception, keystroke logging, malware, unauthorized location tracking, network exploits, phishing, spamming, spoofing, theft or loss, and zero day attacks (GAO, 2012; see Appendix B).

Browser exploits are intended to take advantage of weaknesses in software used to interact with websites. The installation of malware or the performance of other adverse actions on a mobile device can be accomplished through deceptive web pages and associated hyperlinks (GAO, 2012).

Data interception can take place when an attacker is spying on data exchanges originating from or being sent to a mobile device. Data interception can be achieved through various techniques. The man-in-the-middle attack (MitM) can occur when a mobile device joins to an unsecured Wi-Fi network, permitting an attacker to capture and possibly alter data packets between devices (GAO, 2012). The implementation of digital signatures and public key certificates can mitigate this susceptibility (Stalling et al., 2008b, p. 645). The process of an attacker capturing and not discarding data meant for another recipient exchanged over an unencrypted network is referred to as Wi-Fi sniffing (GAO, 2012).

Keystroke logging is a type of monitoring that archives keystrokes on mobile devices in order to appropriate sensitive information. Generally, keystroke loggers transmit the information they capture to a cybercriminal's website or e-mail address (GAO, 2012). Loggers can monitor either software or hardware. Software keystroke loggers can be implemented through a Trojan horse (Harris 2010a). Typical software/anti-malware scanning tools cannot identify a hardware keystroke logger (Walker, 2012a).

National Institute of Standards and Technology (NIST) Interagency Report (IR) 7298 Revision 2 (Kissel, 2012), titled *NIST Glossary of Key Information Security Terms*, defines malware as a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system, or of otherwise annoying or disrupting the victim. Malware can be malicious code, malicious applets, or malicious logic. The *NIST Glossary* (Kissel, 2012) explains that malicious code can be software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of an information system. Examples of malicious code include viruses, worms, Trojan horses, or other code-based entities that infect a

host; this includes spyware and types of adware (Kissel, 2012). The NIST identifies malicious applets as small application programs that are automatically downloaded and executed, and that perform an unauthorized function on an information system (Kissel, 2012). The NIST explains that hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose is malicious logic (Kissel, 2012). Malware can instigate a broad collection of attacks to propagate itself onto other devices in an effort to employ a number of possible functions. These functions include

- accessing location information and other sensitive information,
- obtaining read/write access to the device's browsing history,
- initiating telephone calls,
- activating the device's microphone or camera in an effort to record information, and
- downloading other malicious applications. (GAO, 2012)

Location tracking permits the position of listed mobile devices to be identified and observed. Location data may be gained through valid software applications as well as through malware configured on the user's mobile device. Legitimate tracking can be accomplished with proper authorization and consent. Unauthorized location tracking occurs covertly without the user's knowledge or consent (GAO, 2012).

Harris (2010a) defines phishing as a type of social engineering with the goal of obtaining personal information, credentials, credit card information, or financial data. Phishing can include e-mail or pop-up messages to deceive users into disclosing sensitive information. Attackers employ bait to lure or "phish" for sensitive data through different approaches (GAO, 2012).

3. Key Security Controls for Mobile Devices

Users must take precautions to combat mobile security attacks. No single solution for mobile device security will prevent all of the attacks, but some key controls can help to decrease the likelihood of an attack. Enabling user authentication on the mobile device, such as a lockout pin and password, is considered essential to its physical security.

Thirty-three percent of smartphone users have lost their device or had it stolen at some point (Boyles et al., 2012). With such a high general instance of lost or stolen mobile devices, the ability to remotely disable or wipe a mobile device is critical to safeguarding its content and the network(s) it accesses. Implementing a whitelisting policy for mobile devices, in which only qualified mobile applications can operate on the system, mitigates the spread of malware and minimizes device exploitation. Each precautionary measure taken adds another layer of security to the overall system. However, the incorrect combination of, or use of too many, precautionary measures can prove to be a hindrance to mobile device functionality from a user level.

The process of sending unsolicited commercial e-mail advertising for products, services, and websites is referred to as spamming. With the proliferation of mobile devices, spam is being conveyed in text communications in addition to electronic mail. This can not only impact the user's physical environment by requiring the user to manually delete messages from the devices, but also cause the user to be burdened with additional monetary charges for the unsolicited texted messages. Malicious software can also be delivered through spam or in phishing schemes (GAO, 2012; see Appendix C). Mobile devices' small form factor and their intended usage environment make them inherently simpler to lose or rob than the standard laptop or tablet. Additionally, the efficient hardware design of mobile devices allows for access through multiple points in order to retrieve resident data (GAO, 2012).

Additional security measures can help to implement and manage mobile devices on a network. When an organization implements a centralized security management system of the entire architecture, a holistic view can be achieved. A centralized security management system can validate if an organization's mobile devices are compliant with mandated security policies. The centralized security management system should include configuration control and management permissions. These in particular can disable the ability to install malware to remote devices by individual users or a class of users that may have escalated privileges in an attempt to gain access to specific devices. An organization should include an enterprise firewall configured to isolate all unapproved traffic to and from wireless devices, and it should monitor incoming traffic with an

intrusion detection system (IDS; GAO, 2012; see Appendix D). Automated software tools can provide real-time status reports of a device's compliance and status. Through active and passive scanning for key compromising events (e.g., an unexpected change in the file structure), information professionals can determine risk and formulate mitigation steps (GAO, 2012).

4. Key Security Practices for Mobile Device Users

System security is as strong as its weakest link. In a majority of systems, the user is the weakest link. By following some key security practices, users greatly reduce the overall threat level and vulnerabilities of a system. Public Wi-Fi is often riddled with security vulnerabilities. Thus, limiting contact with public Wi-Fi decreases exposure to possible exploitation (GAO, 2012; see Appendix E). Unknown web links represent a significant threat to mobile device security, and it is a best practice to never click on web links from suspicious e-mail, text messages, or advertisements (GAO, 2012).

The installation of unnecessary software applications, or apps, on a mobile device also increases its potential security exploitation and vulnerability (GAO, 2012). Thirty-eight percent of U.S. adults downloaded apps in 2011 (Boyles et al., 2012). Many of the apps on the market today gather information on the user and pass that information to other sources (Boyles et al., 2012). Fifty-four percent of app users have deleted an app from their device that they feel captured too much of their personal information (Boyles et al., 2012). The mobile industry also acknowledges that the data collection procedures of some apps are not defined well enough. Apple, Google, Microsoft, Amazon, Hewlett-Packard, and Research in Motion have all agreed to provide better app privacy policies to their users (Boyles et al., 2012).

Personal information shared over the Internet should be minimized. When it is necessary, appropriate measures will ensure maximum risk mitigation so that personal information is not compromised. Users should conduct Internet commerce through secure, encrypted connections (GAO, 2012). In addition, limiting the posting of mobile phone numbers on public websites reduces a user's chance of an attack (GAO, 2012).

Mobile device settings play a large role in user security. Mobile devices with a discoverable mode should disable the capability, or set their device to non-discoverable (GAO, 2012). Devices in discoverable mode are visible to other devices in the immediate area and offer attackers an easy target for exploitation.

Maintaining good physical control of a mobile device reduces its chance of being lost or stolen (GAO, 2012). Users should limit the storage of sensitive information and delete all personal information from a mobile device before discarding it (GAO, 2012).

The popular practice of "jailbreaking" mobile devices, which bypasses integrated security and operating system restrictions, frequently results in expanded device capabilities. However, it often voids the warranty of the device and violates the terms of any contracts in place. In addition to legal ramifications, jailbreaking often results in higher security vulnerabilities in mobile devices and should be avoided (GAO, 2012, Scarfone & Souppaya, 2012).

5. Additional Security Practices

Organizations can implement some additional security practices that can help their mobile device users against threats and vulnerabilities. Establishing a mobile device security policy provides a uniform set of rules and practices for the entire organization to follow (GAO, 2012; see Appendix F). Specific security training for mobile devices raises the organization's overall awareness of the subject (GAO, 2012). Being proactive in conducting accurate risk assessments on the state of mobile devices on the network can also help an organization identify, prepare for, and eliminate mobile device attacks (GAO, 2012).

Taking the time to develop a well-thought-out mobile device deployment plan will help an organization meet its IT security objectives (GAO, 2012). Performing centralized mobile device configuration management and control allows for safeguarding against unauthorized modifications of devices within the organization's network infrastructure (GAO, 2012).

D. MOBILE DEVICE SECURITY

Scarfone and Souppaya (2012) list some additional mobile device features that are of particular security concern such as global positioning system (GPS) capability, digital cameras, microphones, support for removable media, and the ability to use the device itself as removable media. Scarfone and Souppaya (2012) recommend that organizations consider all smart devices as untrusted until they are properly secured and able to be monitored continuously while accessing enterprise data and services. An inherent risk is present when using a mobile device on any network that is not controlled by the user's organization. This elevated level of risk can be mitigated through proper encryption and authentication measures (Scarfone & Souppaya, 2012).

System security should be considered during the initial planning process as it is increasingly difficult to address after system implementation (Jansen & Scarfone, 2008). Security professionals are keenly aware that hackers are now tempted to conduct exploits on mobile devices similar to those they would conduct on a traditional computer (Viega & Michael, 2010). Security professionals are seeing mobile devices undergo attacks that were commonplace during the rise of the traditional computer (Rose, 2012). According to Jansen and Scarfone (2008), if mobile devices are not addressed in an organization's security plan, the result will be a higher potential for security infrastructure compromise. The inherent ability of a mobile device to be mobile poses a risk of potential loss of sensitive data. Mobile devices can be located globally and have the ability to reach back to an organization's infrastructure for connectivity, which poses challenges for administration (Jansen, Gavrilla, Séveillac, Heute, & Korolev, 2004). Once out of the normal work environment, users must be trusted to maintain positive control of their mobile devices at all times. The difficulty of mobile device security is compounded by the comparatively short life cycle of mobile devices and their higher cost of security assessment versus traditional network devices (Viega & Michael, 2010).

Android smartphones are built upon the Linux operating system with applications functioning across components through middleware. This middleware is where hackers or those with malicious intent request greater permissions than actually required in order to access other applications to obtain the user's private or corporate data. Liu, Moulic,

and Shea (2010) state that, "Managing such a complicated and diversified equipment inventory is an increasing[ly] demanding task for many businesses."

Individually managing every mobile device in an organization is an option. Aside from a greater amount of time and effort on the part of the information technicians, this approach also has security concerns. The security capabilities present on the average mobile device fall short of the capabilities offered from Mobile Device Management (MDM) software. Often the required password length is short and the standards used for encryption are lacking (Scarfone & Souppaya, 2012). In addition, the management of mobile systems not present in the enterprise is more difficult. It takes additional effort to ensure that these devices are properly updated, patched, and within configuration standards for the organization (Scarfone & Souppaya, 2012).

Security policies must be enforced and monitored for effective enterprise-level security on mobile devices (Liu et al., 2010). Centralized security management streamlines the control, management, and adherence to policy of mobile devices within an organization (Jansen & Scarfone, 2008). Mobile device security and scalability are critical to an organization's success when implementing an enterprise mobility solution (Liu et al., 2010).

Automated tools decrease risk exposure due to misconfigurations encountered during IT provisioning and deprovisioning (Mont & Brown, 2011). Provisioning and deprovisioning are important in managing accounts and access rights on systems. Mistakes may result in system exploitation, including unauthorized access of information and resources, and the misuse of credentials for illegal purposes (Mont & Brown, 2011).

E. MOBILE DEVICE MANAGEMENT

During the 2010 Institute of Electrical and Electronics Engineers (IEEE) Seventh International Conference on E-Business Engineering, Liu et al. (2010) presented research demonstrating that businesses are increasingly over tasked to manage the growing equipment inventory. Additionally, Liu et al. (2010) identified that security policies not only require enforcement, but continual monitoring and updating of the devices' associated applications to safeguard productivity. Mont and Brown's (2011) research into

information assurance management (IAM) investments has shown how automation can reduce the failure points in how IT systems are configured, thereby reducing risk to the enterprise network.

According to Schultz and Shpantzer (2010), constant Internet connectivity is a critical factor in business profitability. Commercial organizations have turned to mobile devices to provide that constant access. Security professionals are seeking mobile device management options capable of the same level of accountability, protection, and management as those available for conventional computer systems (Microsoft, 2006).

Microsoft (2006) and Apple (2012) have integrated some mobile device management features into their network architecture designs and operating systems. Third-party vendors, however, have introduced solutions for MDM systems to provide broader device security and management capabilities (Microsoft, 2006). Key MDM features include provisioning, monitoring, management, security, and support (MaaS360, 2012). The variety and number of controllable capabilities differ among products (Jansen & Scarfone, 2008).

MDM platforms are built on a traditional client-server model achieved through an agent or app on the mobile device. As with traditional management systems, recurring broadcasts take place with managed mobile devices to monitor system configurations to identify unauthorized modification, update security credentials, obtain device log files, provide system updates, and perform other associated functions (Jansen & Scarfone, 2008). Solutions can be mobile device platform specific or can operate across the spectrum (i.e., Apple's iOS, Google's Android, and Research in Motion's BlackBerry). Monitoring mission-critical applications for updates and compatibility is crucial to ensure productivity (Liu et al., 2010).

MDM solutions can be premise- or cloud-based with management conducted in-house through the purchase of site licenses or as a contracted software-as-a-service (SaaS) package. Successful integration of hardware, software, and users depends on the strategic analysis of the business requirements and processes for a comprehensive security plan (Schultz & Shpantzer, 2010).

When determining the appropriate security plan for mobile devices, the NIST recommends an organization make the decision based on the sensitivity of the information and resources, the organization's level of adherence to the security policy, the total costs associated with the decision, the physical locations of their mobile devices, any technical limitations on mobile devices or software being utilized, and the overall organizational compliance with other mandates and policies (Scarfone & Souppaya, 2012). Organizations must remain vigilant and actively follow technological changes and trends in mobile devices, and modify any of their existing policies when necessary (Scarfone & Souppaya, 2012). Additional considerations when choosing a mobile device solution include the architecture of the solution on the network, the user authentication process, the encryption capabilities, the minimum security standards required, and determination and enforcement of requirements adherence (Scarfone & Souppaya, 2012).

An increase in enterprise services used by organizations has spurred exploration into how to integrate them into mobile platforms in an effective manner (LaFranchise, 2012). To succeed, integration should minimize the data received and stored on mobile devices, and applications should be fully functional without a network connection (LaFranchise, 2012). "The basic requirements for such a mobile solution should include the following: 1) timely, robust and easy access to Service-Oriented Architecture (SOA) system, 2) transparency between connected, occasionally-connected, and disconnected modes, 3) loose-coupling system designed to combine services on demand, 4) lightweight application composition and development and, 5) low total cost of ownership." (Natchetori, Kaufman, & Shapiro, 2008, p. 27)

F. MOBILE DEVICE MANAGEMENT EXAMPLE

No comprehensive, standardized criteria establish what MDM systems must do to be considered secure (Rhee, Jeon, & Won, 2012). The core tenants of security are integrity, availability, and confidentiality. Integrity is the detection of any intentional or unintentional changes to transmitted and stored data (National Institute of Standards and Technology [NIST], 2012). Availability is ensuring that users can access resources using mobile devices whenever needed (NIST, 2012). Confidentiality is ensuring that

transmitted and stored data cannot be read by unauthorized parties (NIST, 2012). The level of integrity, availability, and confidentiality determines the level of security of a mobile device.

1. Mobile Device Management Architecture

"[An] MDM system comprehensively manages mobile devices by monitoring their status and controlling their functions remotely using wireless communication technology such as Over-the-Air (OTA) or Wi-Fi, as well as managing the required business resources" (Rhee et al., 2012, p. 353–354). Rhee et al. (2012) outline an MDM system architecture in an enterprise environment and define a five-step system process (see Figure 2).

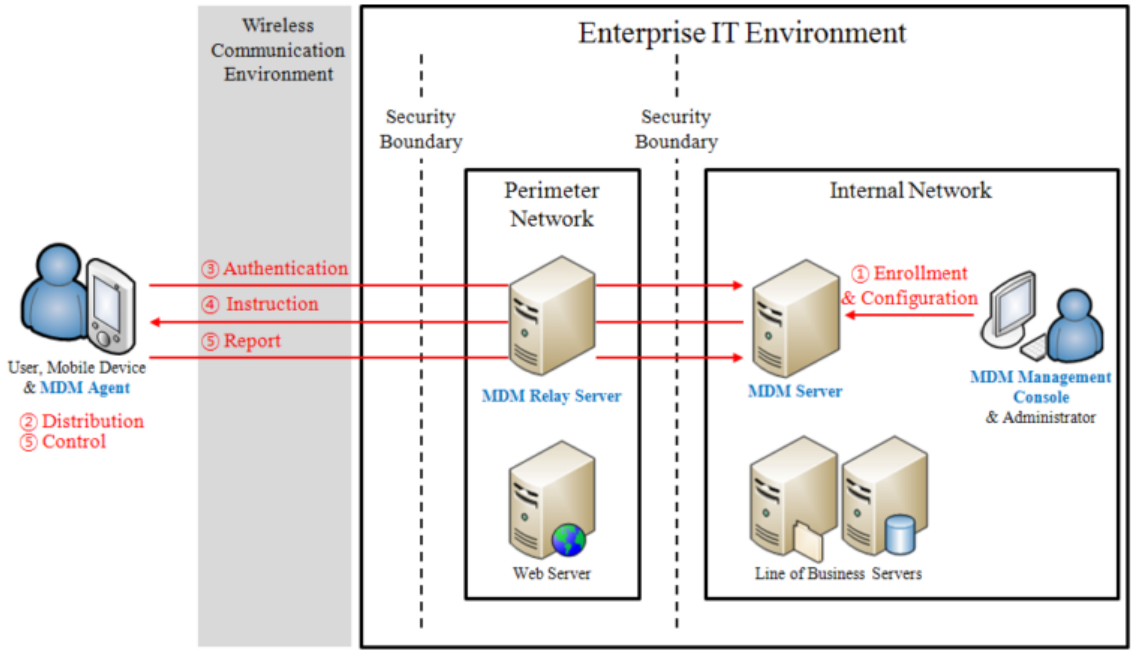


Figure 2. Mobile Device Management System (From Rhee et al., 2012)

The five-step system process outlined by Rhee et al. (2012) is as follows:

Step 1. Enrollment/Configuration: Register the mobile device and user data within the organizational MDM system and configure the device with the appropriate policies.

Step 2. Distribution: Install and distribute the MDM agent on the mobile device. The MDM agent can be distributed through the application store/market or in-house.

Step 3. Authentication: When running the MDM agent, mobile device data (IMEI [international mobile station equipment identity], IP/MAC address, phone number, etc.) travel to the MDM server to verify whether it matches the data registered in the MDM system.

Step 4. Instruction: The MDM server sends the MDM agent on the mobile device control policy and commands.

Step 5. Control/Report: The MDM agent on the mobile device controls its functions according to the organization's mobile device command and control policy. Control measure reports are sent to the MDM server.

2. Mobile Device Management System Threats

Threats exist in MDM systems as they do in any other IT management (ITM) system. Confidential information within the MDM system or the environment in which it operates, or any data transferred between its components, runs the risk of being leaked (Rhee et al., 2012). This is known as disclosure. Software vulnerabilities can open an MDM system to unauthorized modification (Rhee et al., 2012). Risk exists for attackers to bypass security measures to incapacitate or negatively alter an MDM system (Rhee et al., 2012). Attackers may also alter data saved, or transferred by, MDM systems (Rhee et al., 2012).

MDM systems are vulnerable to malware attacks that strike in a variety of forms including viruses, worms, and Trojan horses (Rhee et al., 2012). Attackers can attempt to circumvent the proper authentication protocols by reusing system authentication data to impersonate legitimate users (Rhee et al., 2012). This practice is known as spoofing.

A common practice of attackers is to flood a system or application with traffic to obstruct its normal operation. This is known as a denial-of-service (DoS) attack (Rhee et al., 2012). Another way to inhibit the normal operation of an MDM system is by exhausting the storage available within the system and operational environment with

unwanted data (Rhee et al., 2012). As a result, the MDM system is unable to capture security events and any data vital to the functionality of the system (Rhee et al., 2012).

Not every threat originates from a human source. Natural disasters such as earthquakes, floods, tornadoes, and fires can disrupt MDM systems operations (Rhee et al., 2012).

3. Mobile Device Management Security Objectives

An organization can establish certain MDM security objectives to help mitigate the threats present within the mobile infrastructure. Protecting critical MDM system components through proper network security and a secure physical location is important (Rhee et al., 2012). The operating systems residing on MDM system components should receive regular updates to correct vulnerabilities and be free of any unneeded or untrusted services (Rhee et al., 2012).

Organizations must choose MDM system administrators carefully. They should not harbor any malicious intent or ill will towards the organization and should be trained properly (Rhee et al., 2012). An MDM system should capture and track any security events and allow for updates to the system to fix vulnerabilities and shortcomings in performance (Rhee et al., 2012).

An MDM system should protect saved data from unauthorized viewing, deletion, or change (Rhee et al., 2012). One way to safeguard data transferred over an MDM system is by using secure communications channels between system components (Rhee et al., 2012). An organization should offer secure enrollment of mobile devices and users to its MDM system (Rhee et al., 2012). Only authorized users on approved mobile devices should receive the MDM agent over a secure channel (Rhee et al., 2012).

Once a user is enrolled in the MDM system and the user's device contains the MDM agent, proper information assurance (IA) should be in place to properly authenticate and identify a device's activity (Rhee et al., 2012). If a device fails authentication, a follow-up function should be in place through the MDM system (Rhee et al., 2012). Only authorized system administrators should change MDM system and

mobile device security settings (Rhee et al., 2012). MDM system administrators should receive user and mobile device status data to monitor for unauthorized activity (Rhee et al., 2012).

MDM systems should be able to remotely update mobile devices with security updates and restrict access if devices or users are out of compliance with operating procedures (Rhee et al., 2012). User and functional data should be completely deleted from MDM system functional areas after a session is terminated (Rhee et al., 2012).

Only pre-approved applications should be installed on mobile devices and MDM system components (Rhee et al., 2012). In addition, only authorized processes should be allowed for execution on mobile devices (Rhee et al., 2012). An MDM system should also contain some sort of malware identification and protection (Rhee et al., 2012). Unauthorized change or removal of the MDM agent should be detectable by the MDM system (Rhee et al., 2012). The ability to detect unauthorized changes to the MDM system or operational environment is also important (Rhee et al., 2012).

G. MOBILE DEVICE MANAGEMENT IN A CLOUD ENVIRONMENT

Manufacturers of mobile devices often provide little software support for their products (Ruebsamen & Reich, 2012). For security purposes, it is important to identify vulnerabilities in software and install updates as needed, especially in the operating system of a device (Ruebsamen & Reich, 2012). The emergence of cloud computing is allowing for centralized storage and synchronization across many devices (Ruebsamen & Reich, 2012). Ruebsamen and Reich (2012) suggest that cloud computing allows resource-intensive applications to run on mobile devices without the restriction of residing on the individual device. A proxy server located in the cloud can determine what devices are granted access to the available content (see Figure 3).

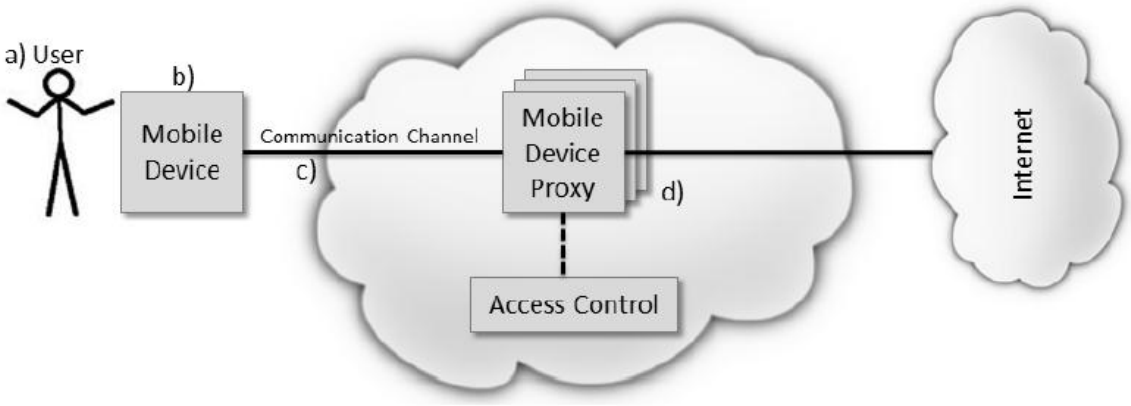


Figure 3. Mobile System Architecture With Cloud Proxy
(From Ruebsamen & Reich, 2012)

The security of the entire framework is based on the security and trust relationship between the user, the mobile device, the channel over which communications are taking place, and the proxy server (Ruebsamen & Reich, 2012).

Ruebsamen and Reich (2012) suggest assigning a security level of 0–4 to individual mobile devices (see Figure 4). Level 0 means that a device is critically unsecure and Level 4 is assigned to devices that are highly secure (Ruebsamen & Reich, 2012). The proxy server scans each mobile device to determine the level of security it resides at. The security level system determines the content that individual mobile devices can access through the proxy server.

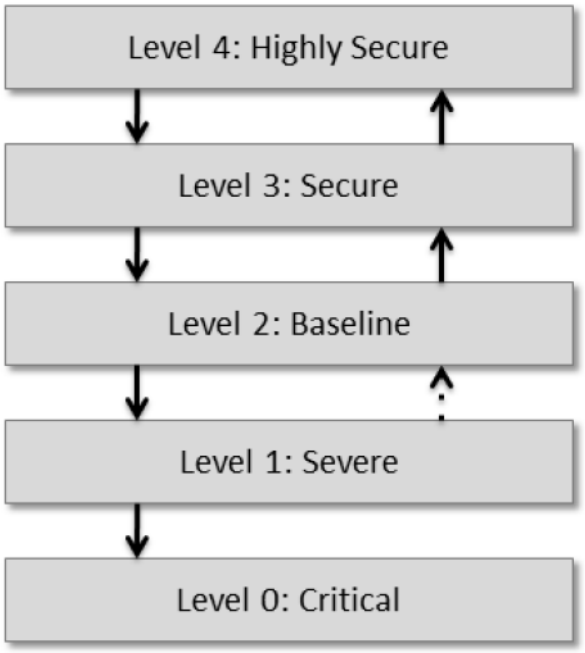


Figure 4. Security Levels (From Ruebsamen & Reich, 2012)

H. BRING YOUR OWN DEVICE

The increase of mobile device usage and capabilities is stimulating the "consumerization" of IT. Regard (2012, p.10) describes consumerization as "[t]he purchase of devices by employees who then petition IT to allow their integration into the corporate systems." Users become attached to their smart devices, and it is often hard to get them to switch to another type of device (Miller, Voas, & Hurlburt, 2012). Consumerization and organizational cost savings are main motivators behind the concept of bring your own device (BYOD).

BYOD refers to employees using personal mobile devices in a business capacity (Avema Critical Wireless, 2011). Eighty-three percent of U.S. adults own a cell phone, and 42 percent of those cell phones are smartphones (Rose, 2012). Many commercial corporations have capitalized on this fact and stand at the forefront of integrating mobile devices into their organizations' infrastructure. They realize that the reduction of hardware costs is a significant advantage (Schultz & Shpantzer, 2010). In 2012, 95 percent of U.S. organizations permitted personally owned smart devices in the workplace (Miller et al., 2012).

Many organizational networks contain mobile devices that are self-administered by end users (Schultz & Shpantzer, 2010). This allows end users control over device settings in such areas as application and program installation, and configuration of the operating system (Schultz & Shpantzer, 2010). Most mobile device architectures complement a user's ability to self-administer.

I. THE DEPARTMENT OF DEFENSE AND MOBILE DEVICES

The DoD CIO's (2012, p. 1) mobility vision is "[a] highly mobile workforce equipped with secure access to information and computing power anywhere at any time for greater mission effectiveness."

MDM systems are utilized in an effort to mitigate the myriad mobile device risks facing organizations. The DoD CIO is proceeding with a mobile device strategy that includes the establishment of an MDM service in an effort to "advance the operational effectiveness" of the DoD enterprise network (DoD CIO, 2012). Goal 1 is to advance and evolve the DoD information enterprise infrastructure to support mobile devices. Goal 2 is to institute mobile device policies and standards. Goal 2's second objective is to establish an MDM service. Goal 3 is to promote the development and use of DoD mobile and web-enabled applications.

The U.S. Communications-Electronics Research, Development, and Engineering Center (CERDEC) summarizes research conducted with the use of commercial phones in an Army brigade unit by highlighting that, while technically feasible, researchers are not including network management requirements into the overall network model (Kaul, Makaya, Das, Shur, & Samtani, 2011). This is in direct opposition to Objective 3 (establish a mobile device security architecture) of Goal 1 of the DoD CIO's Mobile Device Strategy.

Most mobile devices are equipped with 802.11 capabilities that allow them to connect to ad-hoc networks. Mobile Ad-hoc Networks (MANETs) contain mostly lightweight devices that possess minimal capabilities (Toubiana & Labiod, 2008). Security management is crucial to the efficient performance and resource use in MANETs (Toubiana & Labiod, 2008). In recent experiments, researchers have presented

“a deployment architecture and use cases for commercial smartphones to be used in a heterogeneous environment that includes expeditionary cellular, ad-hoc wireless and indigenous cellular networks as well as smartphones connecting to traditional military radios over other native interfaces” (Kaul et al., 2011, p. 2205). The results from these experiments highlight the fact that, while technically feasible, researchers are not including device management architecture in the network model.

Simple Certificate Enrollment Protocol (SCEP) is an Internet draft staffed with the Internet Engineering Task Force (IETF) and developed as a joint venture by Microsoft, Cisco, and VeriSign. It is intended to simplify the distribution of certificates during large-scale deployments of mobile devices for network enrollment (Apple, 2012). In public key cryptography, the association between individual identities and their public keys must be authenticated in a secure manner (Liu, Madsen, & McDrew, 2002). This process prevents man-in-the-middle attacks in which data is manipulated by an unwanted party as it travels between the sender and intended recipient (Liu et al., 2002). Dense MANETs are prime targets for hackers and should be secured appropriately (Toubiana & Labiod, 2008).

A possible solution for the security of mobile devices outside of a garrison environment, in deployed or emergency situations, exists through mobile security enclaves. These enclaves control access to network assets on an individual device level based on specific conditions (LaFrenier, 2011). A test application is run to determine if the device is connected to specific cellular or Wi-Fi base stations, or is located within a certain geographical location based on GPS coordinates (LaFrenier, 2011). If the application is passed, authentication between the mobile device and security enclave is conducted. This can be accomplished through the traditional exchange of keys. Once the authentication takes place, the mobile device has access to the specified content within the security enclave.

J. INFORMATION TECHNOLOGY ACQUISITIONS

The DoD's total IT budget for fiscal year (FY) 2012 was $38.5 billion (Defense Budget Board, 2012). Its IT infrastructure has over 6,000 locations, 15,000 networks, 3,000,000 users, and 7,000,000 IT devices (Defense Budget Board, 2012).

When dealing with the acquisitions of IT systems, initial costs include staff, hardware, software, and enterprise purchases. Follow-on costs include support and maintenance, suboptimal staff utilization, and underutilization of client and support hardware (Defense Budget Board, 2012). An IT acquisition plan must take into account the entire mobile device life cycle. A mobile device life cycle consists of five phases: initiation, development, implementation, operations and maintenance, and disposal (Scarfone & Souppaya, 2012).

It is critical to factor in enterprise architecture (EA) when making IT investments (GAO, 2004). The GAO (2004) outlines five maturity stages in IT investment. Each stage has critical processes that have to be met to progress to the next stage of maturity. Based on an organization's individual circumstances, the framework can be applied in a unique manner to effectively guide the information technology investment management (ITIM) process. The guide also serves as an assessment tool for performance of ITIM and identification of areas of improvement. The GAO (2004) outlines some specific areas that the framework applies to, as follows (see Figure 5):

- investment management,
- strategic planning,
- software/system development and acquisition management,
- IT services acquisition management,
- human capital management,
- information security management, and
- enterprise architecture management.

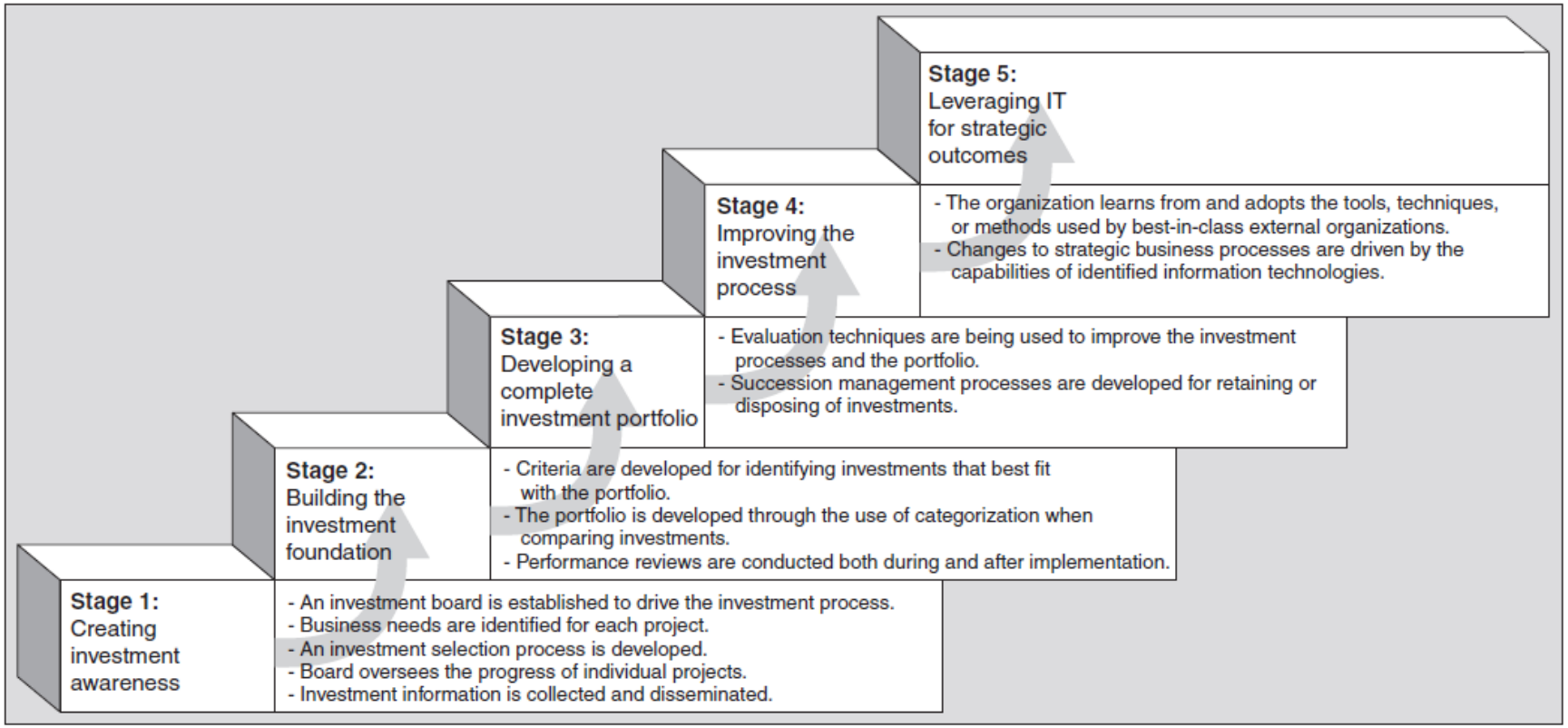


Figure 5. Critical Maturation Steps Required to Move to the Next Stage (From GAO, 2004)

The GAO (2011) examines seven successful IT acquisitions within the federal government and identifies common factors that contribute to program success (see Table 1). The GAO (2011) identifies nine common factors as being critical to the success of the IT programs:

1. Program officials were actively engaged with stakeholders;
2. Program staff had the necessary knowledge and skills;
3. Senior department and agency executives supported the programs;
4. End users and stakeholders were involved in the development of requirements;
5. End users participated in testing of system functionality prior to formal end user acceptance testing;
6. Government and contractor staff were stable and consistent;
7. Program staff prioritized requirements;
8. Program officials maintained regular communication with the prime contractor; and
9. Programs received sufficient funding.

Of the nine common factors to successful IT acquisitions programs, having program officials actively engaged with stakeholders is a critical success factor in all seven of the programs analyzed.

Table 1. Commonly Identified Critical Success Factors Across Seven Successful IT Investments (From GAO, 2011)

		Investments						
Critical success factors		**DRIS**	**GCSS-J**	**MOMentum**	**WHTI**	**ITWS**	**CADE 2**	**OHRS**
1	Program officials were actively engaged with stakeholders.	X	X	X	X	X	X	X
2	Program staff had the necessary knowledge and skills.	X		X	X	X	X	X
3	Senior department and agency executives supported the programs.	X	X		X	X	X	X
4	End users and stakeholders were involved in the development of requirements.	X	X	X		X		X
5	End users participated in testing of system functionality prior to formal end user acceptance testing.		X	X	X	X		X
6	Government and contractor staff were consistent and stable.	X	X		X	X		
7	Program staff prioritized requirements.		X	X		X		X
8	Program officials maintained regular communication with the prime contractor.	X		X	X			X
9	Programs received sufficient funding.	X			X		X	

K. LITERATURE REVIEW SUMMARY

MDM is not a new concept, but it has yet to achieve widespread implementation. A limited amount of research and studies exist on the subject. The inclusion of mobile devices in an organization's enterprise architecture (EA) framework have IT professionals seeking MDM solutions in order to mitigate security concerns and provide oversight on mobile infrastructure. With no clear MDM standards defined, the DoD faces a challenge in determining which MDM solutions best fit its organizations.

III. EVALUATING MOBILE DEVICE MANAGEMENT SOLUTIONS

A. ENTERPRISE ARCHITECTURE LINK TO OPERATING MODEL

Operating models are important with respect to an organization's enterprise architecture (EA) design to maximize business process efficiencies. Ross, Weill, and Robertson (2006a) identified the fundamental characteristics of the four types of operating models (see Figure 6). The GAO and Ross et al. both define the EA in similar terms, highlighting the need to merge business core functionality with information technology (IT) to maximize those efforts. Ross et al. (2006a, p. viii) explain that the EA "is the organizing logic for business process and IT infrastructure reflecting the integration and standardization requirements of the company's operating model."

Merging business processes with technical innovation allows for the creation of current and future EA views (Shirazi, 2009). Nonspecific government-based models for an EA are available for reference. Bologa, Faur, and Ghisoiu (2010, p. 19) present a standard model composed of four fundamental components: "the architecture of the business models and processes, the software architecture that would support business processes, the architecture of the information and data that are used or obtained …, and the technology architecture suitable for achieving the objectives." Schuck (2010) describes the EA as a "business system" that maps the overlapping line of influences by critical stakeholders that results in a practical resolution. Stakeholders achieve this with end-to-end communication of planning systems and data stores allowing for swift reaction to current information (Schuck, 2010).

What is often overlooked is that different EAs operate within a complex organization (Ross et al., 2006a). Data requirements for each level are also different (Bologa et al., 2010). Data gathered at one level may not be needed at higher levels, whereas linkages between data points in different process streams are relevant. Alignment of business processes can be achieved through bottom-up analysis of data threads that confirm top-down business models' data requirements are met (Bologa et al., 2010).

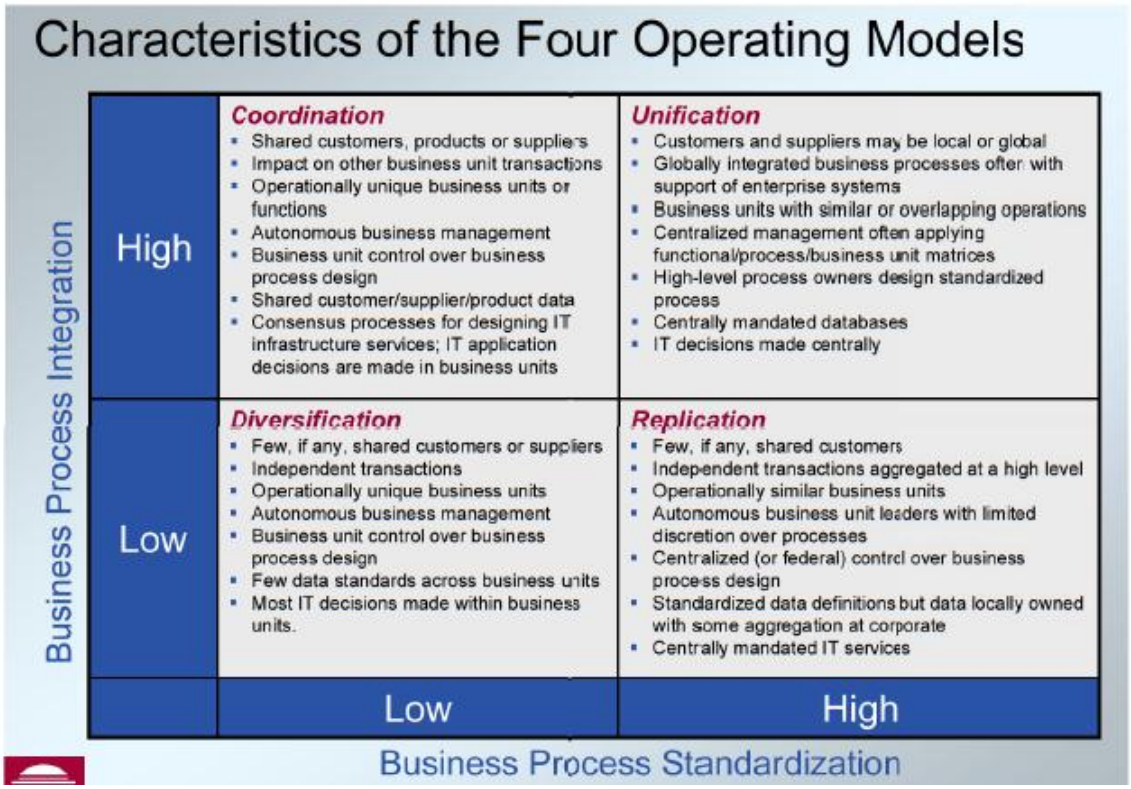


Figure 6. Four Operating Models (From Ross et al., 2006b)

1. Chief Information Officer Role Linked to Architecture Maturity Model

The term chief information officer (CIO) first came about in the private sector in the early 1980s with the expansion of information technology into the business workplace (Banker, Hu, Pavlou, & Luftman, 2011). The role of the CIO was to act as a bridge between the information technology section supporting the core processes of the business and corporate-level (C-Level) executives (Hunter, 2011). In the private sector, the chief executive officer (CEO), the chief operations officer (COO), the chief financial officer (CFO), and the CIO build the core management team of an organization (Dawson & Kauffman, 2010). The public sector does not use the titles CEO, CFO, or COO, but comparative positions correlate respectively (Dawson & Kauffman, 2010; Durmusoglu, 2009). The title CIO did not exist within government until 1996 with the enactment of the Clinger–Cohen Act (1996). The private sector has seen the CIO's role increase into C-level leadership, growing from initial responsibilities of overseeing data processing, then

expanding to corporate-wide resourcing, and, finally, becoming today's strategic-level business integrator (Hunter, 2011). Ross et al. (2006a) identified the four stages of architecture maturity as "a fairly predictable path to achieve a foundation for business execution and follow a consistent pattern for building out [an organization's] enterprise architectures" (see Figure 7).

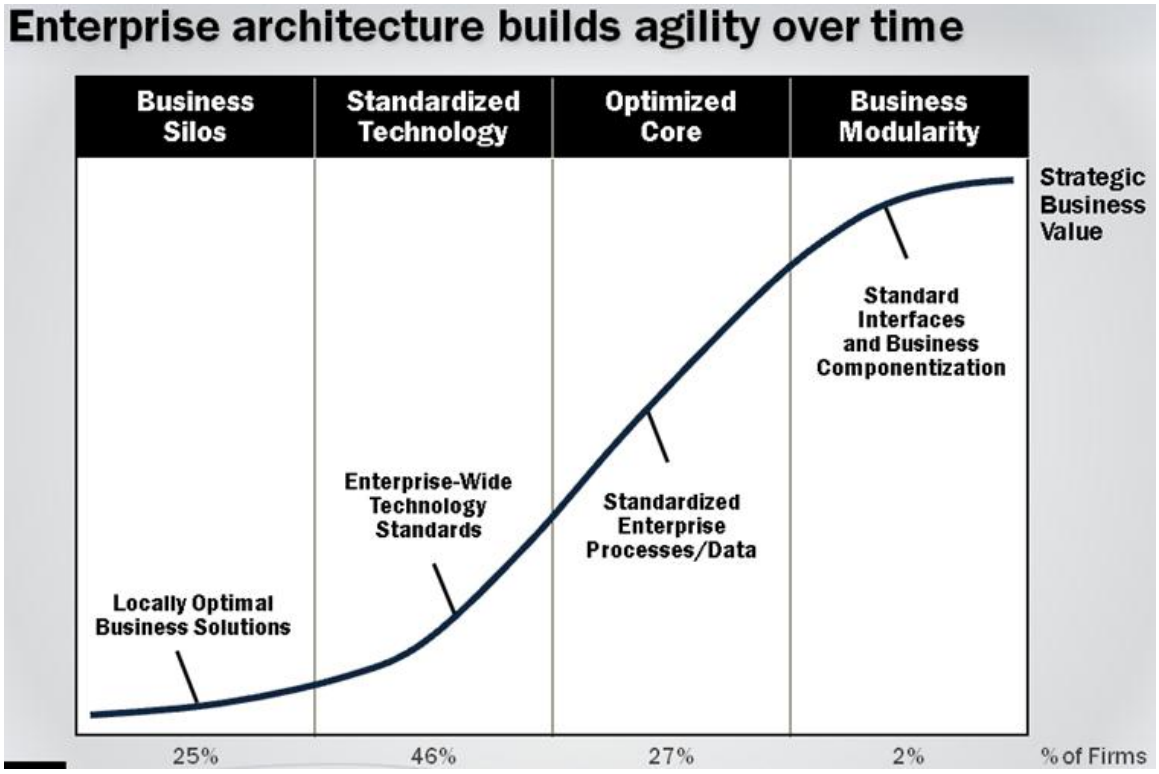


Figure 7. Enterprise Architecture Agility Over Time (From Ross et al., 2006c)

2. Business Silo Stage

Ross et al. (2006a) characterized companies at this stage as attempting to maximize individual business units' needs or functional needs. The role of a CIO in the private sector is influenced by the reporting structure that the company creates (Banker et al., 2011). The two most common organizational models are for the CIO to report to the CEO or CFO (Banker et al., 2011). This is typical during the business silo stage of the architecture model (Ross et al., 2006a). The hierarchal structure that a company establishes has implications for the overall performance of the company through its effect

on the core management team's interaction and decisions regarding IT long-term strategic initiatives (Banker et al., 2011). A CIO must be no more than two levels below the CEO in order to influence decisions (Banker et al., 2011). The Clinger–Cohen Act of 1996 created the title of CIO. Individual organizations' CIOs were quickly established. The first overarching federal CIO was not appointed until 2009 (The White House, Office of the Press Secretary, 2009). The federal CIO directs the policy and planning of federal IT investments, provides oversight on federal IT spending, establishes and oversees the federal EA, and ensures IT privacy and information security throughout the government (The White House, Office of the Press Secretary, 2009).

During this initial stage, companies are designing business processes with CIOs focusing on IT functionality (Ross et al., 2006a). Business strategies are fixated on investments that will bring profits in the short term (Ross et al., 2006a). This is the traditional supply-side role of CIO leadership in which a CIO's technical knowledge builds an IT foundation aligned to support the business processes (Chen, Preston, & Xia, 2010). A private-sector CIO who continues to focus on only standard enforcement and integration of systems may not have the skill set to move the company to the next stage, or the company may outgrow the CIO (Chen et al., 2010). The CIO's role in the public sector is more standards-focused than in private industry due to the government being a non–revenue-generating business (Fortino, 2008).

3. Standard Technology Stage

Ross et al. (2006a) characterized this stage as one in which companies provide IT efficiency through technology standardization and, in most cases, increased centralization of technology management. Shared infrastructure is the critical step in beginning this stage (Ross et al., 2006a). At this stage, organizations begin to share data, but business data require specific applications in order to utilize the information (Ross et al., 2006a). The federal government is in the early stages of this process, with the DoD lacking the details needed to execute the strategy (GAO, 2007). The CIO must effectively manage an IT budget to resource projects (Ross et al., 2006a). Within the DoD, the DoD (2010) Architecture Framework Version 2.02 (DoDAF) supports the CIO in development of the

maintenance of architectures as mandated by the Clinger–Cohen Act (1996). Corporate-level risk management, change management, and problem solving are required in the CIO's skillset toolbox (Hunter, 2011). Demand-side leadership traits become more critical for solving business needs and generating business opportunities with IT solutions (Chen et al., 2010).

The CIO's reporting requirements typically shift to the CEO as the organization's priority shifts from risk management, which is a CFO purview, to alignment to business goals, which is a CEO purview (Ross et al., 2006a). Government agencies have shown greater division of power and increased requirements to conform to administrative processes when compared to private businesses (Dawson & Kauffman, 2010). Recruiting technology staff for the government has become more difficult due to a lack of interest in working for the government (Dawson & Kauffman, 2010).

4. Optimized Core/Business Modularity Stage

When a company views data and applications at an enterprise level, instead of a singular level, it is at an optimized core stage of development (Ross et al., 2006a). Ross et al. (2006a) identify that with a business modularity architecture, a company manages and reuses loosely coupled IT-enabled business process components to preserve global standards while enabling local differences. In essence, data and applications are captured at an enterprise level with the IT allowing for predictable core processes (Ross et al., 2006a). During this culminating stage, an organization's IT systems are able to produce services in the form of data that are in turn consumed by the business organization (Prohaska, 2011). Innovation and knowledge management have further expanded the CIO role (Hunter, 2011). CIOs are primarily organizational leaders that at the strategic level are leveraging technology not only to meet the business' future needs but also to ensure it obtains and maintains a competitive advantage (Fortino, 2008). The CIO is required to have an organizational vision of how IT can allow growth and provide a competitive advantage (Chen et al., 2010). CIOs are not required to be the technical experts, but must effectively interact with C-Level executives so they can influence decisions related to aligning technology with the organization's mission and vision (Fortino, 2008).

At this stage, other C-Level executives rate the CIO's effectiveness to lead the organization in exploring IT modernizations and strategic prospects (Chen et al., 2010). Quantifying success for the CIO at this stage, the private and public CIO are often at polar opposites. The private sector defines return on investment (ROI) as net profit divided by investment, while the government defines ROI as benefit divided by cost (Whitehead, Sarkani, & Mazzuchi, 2011). Success for the public CIO is contingent upon reducing cost while improving performance (Whitehead et al., 2011).

5. Role of Enterprise Architecture

An EA is not limited solely to the IT assets, but also comprises the business practices that make up the core of the organization in its current state as well as its future. Business strategies are often focused on investments that will bring profits in the short term (Ross et al., 2006a). Companies have realized that the steady rise in IT investments is a crucial strategic building block in the success or failure of their organizations that must be properly managed (Durmusoglu, 2009). Today's web-like model requires high integration of business process data, while organizations must also seek consensus for designing an autonomous IT infrastructure within the business units for IT applications. This allows for business unit agility. Business units are able to seek a competitive advantage through an innovation within their business unit or restructure as needed in response to innovations within the ecosystem (Kelly, 2003). The federal CIO role continues to evolve in line with the architecture maturity model with greater responsibility and involvement as the federated architecture of the United States matures. DoD CIO skill sets will have to grow from those of the technical guru to those of the innovator who is able to motivate change at the strategic level. The DoD CIO's roles and responsibilities will sequentially evolve, requiring de-confliction from other governmental agencies in order to remove duplication of efforts and align strategic initiatives with the government's long-term goals. Government policy and official guidance will be required to effect the organizational change required to overcome the administrative processes in the federal system.

In conclusion, the DoD must align integration and standardization concepts as outlined by the operating models with the web-like value chain. To accomplish this, the DoD must transition to a coordination operating model in order to achieve an adequate level of process integration and standardization of data to leverage today's network economy. The EA will denote the information systems executing the core missions of the DoD business units and mitigate risks. The end state will allow the DoD to be more agile with lower risk, yet provide increased capabilities through partnered successes.

B. SYSTEM EVALUATION

In *Government Use of Mobile Technology: Barriers, Opportunities, and Gap Analysis* (Digital Service Advisory Group & Federal Chief Information Officer's Council, 2012), the Digital Service Advisory Group and the Federal Chief Information Officer's Council identify four top mobile challenges (see Figure 8). The number one mobile challenge identified is Mobile Device Management.

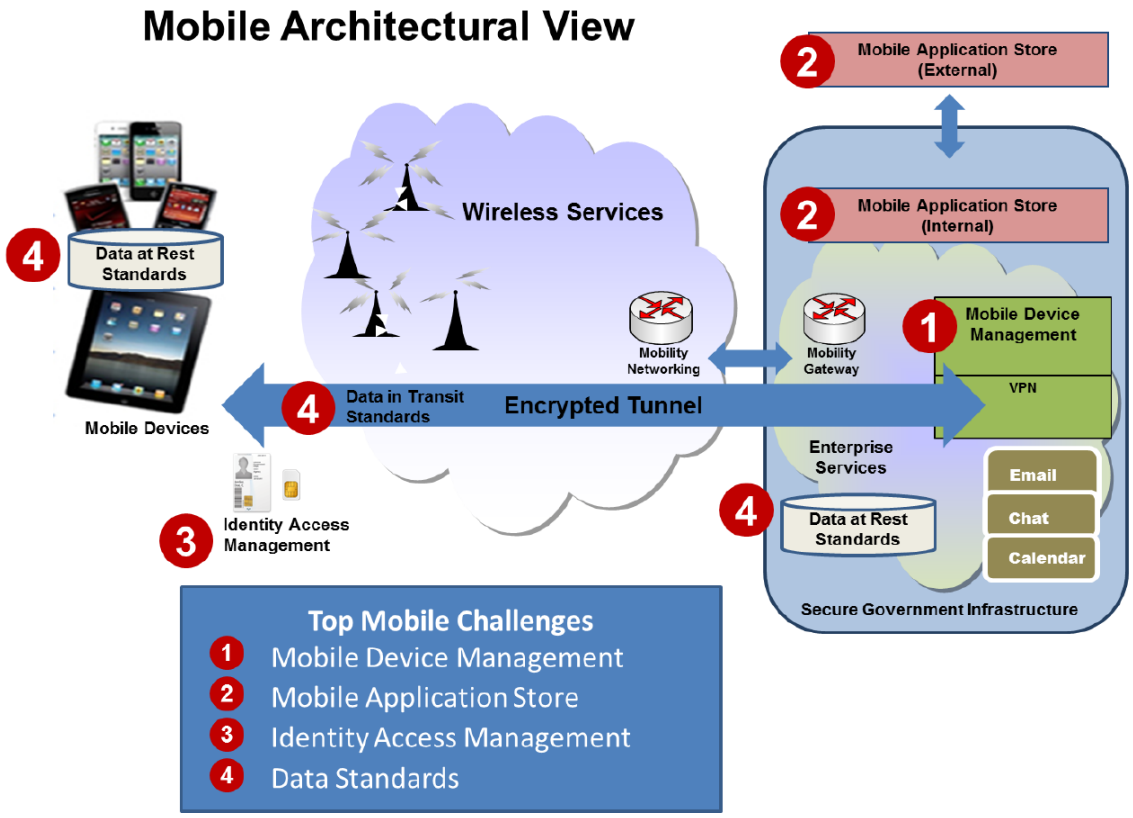


Figure 8. Top Federal Mobile Challenges (From Digital Service Advisory Group & Federal Chief Information Officer's Council, 2012)

The DoD Systems Management College (2001) defines a system as "an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective." To start the system evaluation process, one must first identify the stakeholders: those groups or individuals who hold influence over, or are influenced by, Mobile Device Management solutions.

1. Identify Stakeholders

To identify stakeholders, researchers must ask the question, "Who are those groups and individuals who can affect and are affected by the achievement of an organization's purpose?" (Freeman, 2010, p. 54). The organization is the DoD, and its purpose is the implementation of an MDM solution. After identifying the stakeholders, their level of importance must be determined. To determine the importance of a stakeholder, an evaluation can be conducted using the power/interest grid (see Figure 9).

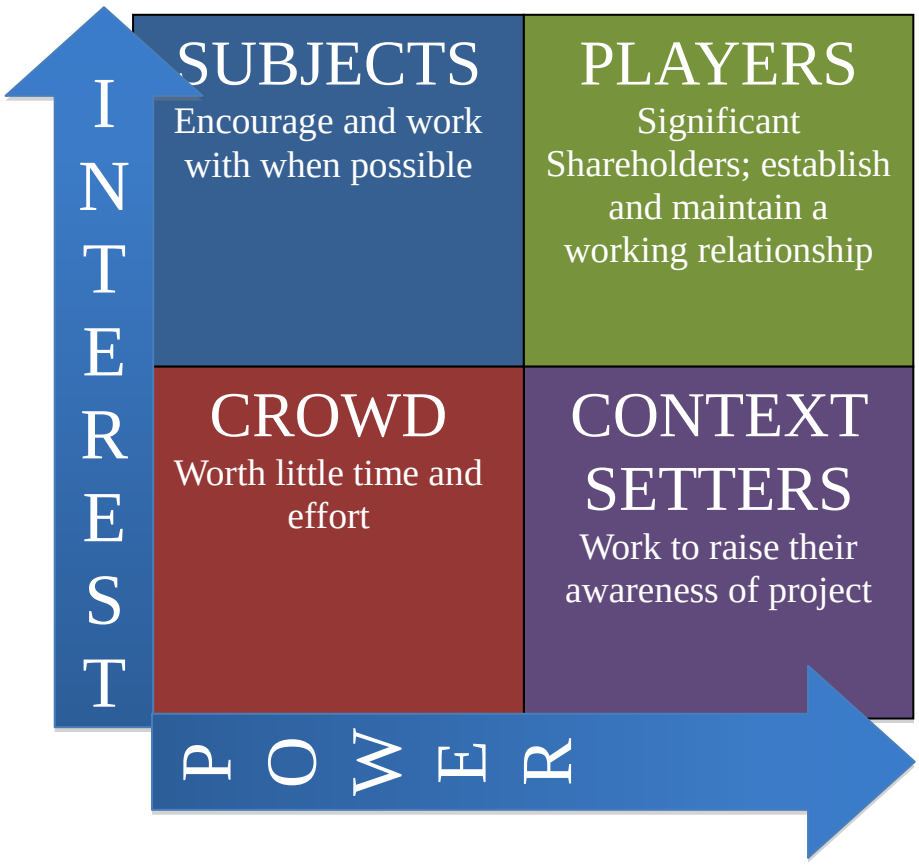


Figure 9. Power/Interest Grid (After Ackermann & Eden, 2011)

In addition to the identification of stakeholders, their management is also important. Each potential stakeholder is evaluated on the levels of power and interest they have in the project. Based on their levels of power and interest, they are grouped into one of four categories (Ackermann & Eden, 2011):

- Crowd—have low power and interest in the project and warrant little time and effort on the part of the managers
- Context Setters—hold the potential for significant power in the project, but have low interest in it; raising their awareness in the project could increase their interest in it
- Subjects—are interested in the project, but have little power over it; providing encouragement and aligning other stakeholders with them can increase their power

- Players—hold both a high level of power and interest in the project and are considered significant stakeholders; quickly establish a good working relationship with them and maintain this relationship for the duration of the project

2. Stakeholder Objectives

After determining the importance of the stakeholders, the significant stakeholders are solicited for their objectives regarding MDM solutions. While several stakeholders exist for the implementation of MDM solutions within the DoD, there are only a few significant stakeholders at this point in time. MDM is a fairly new concept and does not have a baseline set of standards from which it can be evaluated. In addition, few stakeholders have the requisite knowledge of MDM to draw from to solicit quality objectives. The researchers have identified IT and acquisitions professionals within the DoD as two significant stakeholders in the DoD's implementation of MDM solutions. Therefore, this research draws heavily from DoD IT and acquisitions professionals.

3. System Requirements

At this point in the research, individual system requirements are formulated. When formulating a list of good system requirements, there are some key attributes to keep in mind. A good requirement is achievable; verifiable; unambiguous; encompassing of the customer's needs; able to answer the why and what, but not how; consistent with the other requirements; and not too detailed as to constrain available solutions (DoD Systems Management College, 2001)

When combined, all of the system requirements should facilitate the fulfillment of the stakeholder objectives. The accurate capture and representation of the stakeholder objectives and system requirements are essential to the success of any information technology project.

4. Cost Effectiveness Analysis Model

To address the challenge of implementing a MDM solution, the researchers offer a four-tier cost effectiveness analysis (CEA) model to evaluate MDM solution alternatives (see Figure 10).

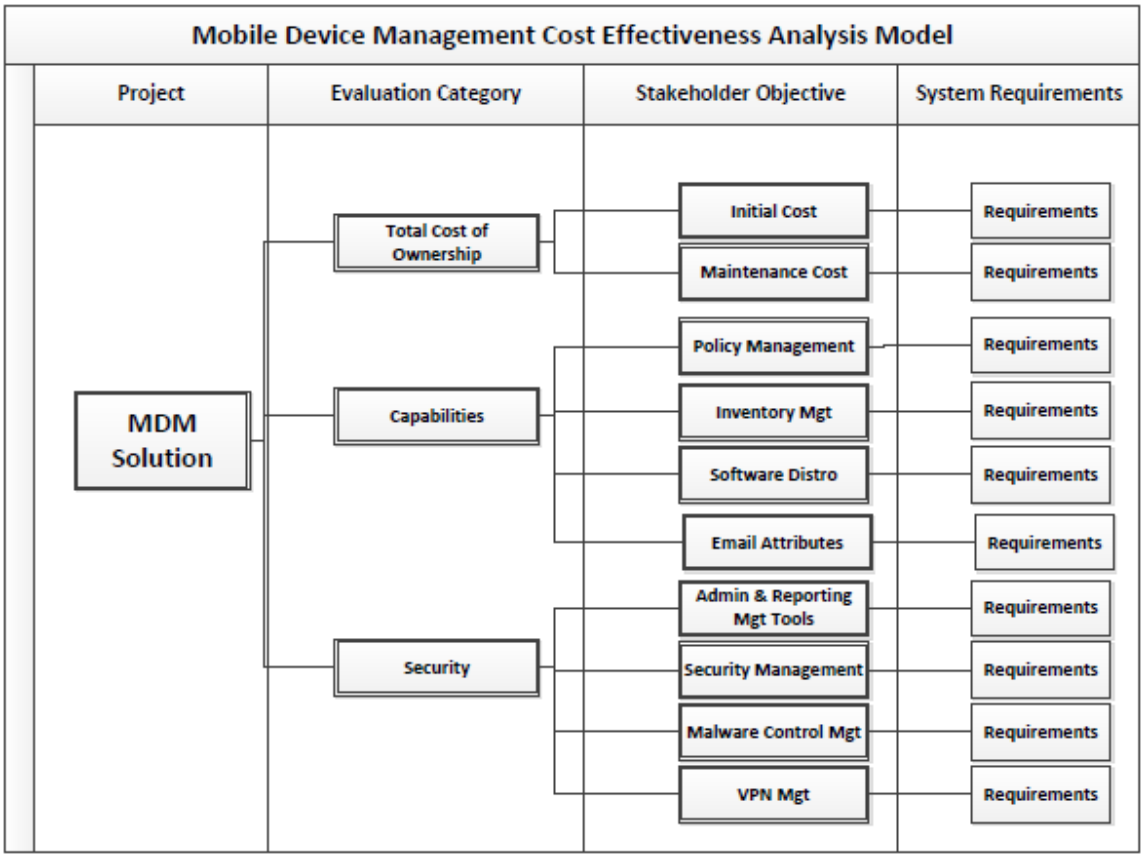


Figure 10. MDM Cost Effectiveness Analysis Model

When the requirements are compiled, they should be grouped into logical evaluation categories. The Federal CIO Council (2009) uses the evaluation categories of capabilities, cost, and security. For the DoD MDM, the researchers present the evaluation categories of capabilities, total cost of ownership (TCO), and security. Each stakeholder objective is aligned under an evaluation category. The researchers align initial cost and maintenance cost under total cost of ownership; policy enforcement, inventory management, software distribution, e-mail attributes, and administration and reporting management tools under capabilities; and security enforcement, malware control management, and virtual private network (VPN) management under security. Each individual system requirement will nest under its applicable stakeholder objective.

This outline forms the basis for the evaluation of potential mobile device management solutions using a CEA model. Weights are assigned to each evaluation category based on importance, with their sum equaling 1.0. Under each category, the applicable stakeholder objectives are also assigned a relative weight based on importance, with the sum of every category's objectives equaling 1.0. This same process applies to each system requirement under all of the stakeholder objectives.

When all of the weights have been assigned to each level of the model, the individual system requirements can start to be evaluated for the available alternatives. If the model is set up correctly, the system requirements should be the only items individually evaluated in the available alternatives. The requirements data collected on each alternative is input into the base level and feeds through the model, culminating in an output between 0 and 1.0. The closer to 1.0 an alternative scores, the better it fits the given situation. It is important to determine the relative weights assigned to each evaluation category, stakeholder objective, and system requirement before analyzing any alternatives.

a. Deployment Environment

Deployment environment is not addressed in the MDM CEA model. However, it is a critical factor in the evaluation of alternatives. Whether enterprise or tactical, the primary environment in which a MDM solution is deployed directly influences its requirements.

C. MOBILE DEVICE MANAGEMENT EVALUATION REVIEW

Enterprise architecture, stakeholders, objectives, and requirements are taken into account when evaluating MDM solutions. A CEA model allows the comparison of various alternatives. Each alternative receives a value, which allows for easier comparison and ranking.

IV. SURVEY DESIGN/IMPLEMENTATION RECOMMENDATIONS

A. INTENDED AUDIENCE

The acquisition and implementation of projects is an arduous process. Understanding project requirements from both a technical and fiscal perspective increases the chances for success. The researchers believe that you must determine the most critical factors when comparing alternatives in order to choose the best possible MDM solution for an organization. It is for this reason that the survey is designed to solicit information from federal IT and acquisitions professionals with knowledge and experience in MDM. This population should provide the most relevant and unbiased data possible while avoiding conflicts of interest or contractual challenges that arise by allowing contractors to participate.

There are federal organizations that contain a concentration of individuals who meet the previously mentioned selection criteria. They include, but are not limited to the following: the Defense Information Systems Agency (DISA); the Department of Homeland Security (DHS); the National Institute of Standards and Technology (NIST); U.S. Army Research, Development, and Engineering Command (USA RDECOM); Communications-Electronics Research, Development, and Engineering Center (CERDEC); the MITRE Corporation (MITRE); and the National Security Agency (NSA). These organizations' missions relate directly to the technical evaluation and planning of IT networks and hardware, and the application of networks and hardware.

The DISA's purview traverses full spectrum operations from joint warfighters with coalition partners to national-level leaders. The DISA delivers, controls, and certifies mission command systems and information sharing capabilities on a global scale. The DISA's concept of the enterprise infrastructure is the backbone for users to join, communicate, and cooperate globally in an effort to more quickly incorporate technology and capability (Defense Information Systems Agency [DISA], 2013).

The NIST's mission is to stimulate U.S. invention and industrial viability through the advancement of science, standards, and technology, addressing improvements to quality of life while boosting economic stability. The NIST's information technology focus hastens the maturity and utilization of systems that are dependable, functional, interoperable, and secure. The goal of the NIST's mobile security and forensics program is to advance the security of mobile devices and software (NIST, 2013).

USA RDECOM seeks to safeguard the warfighter through the exploration and advancement of solutions proven to fill capability gaps identified through the acquisition process. Specifically, CERDEC improves and incorporates command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) technologies into the enterprise architecture (Communications-Electronics Research, Development, and Engineering Center [CERDEC], 2013). The Space & Terrestrial Communications Directorate is involved with MDM in reference to MANET research.

MITRE is a not-for-profit organization with knowledge and expertise in areas such as systems engineering, information technology, operational concepts, and enterprise modernization. MITRE is funded by government sponsors in order to provide solutions for critical requirements. Serving as a federally funded research and development center (FFRDC), the National Security Engineering Center (NSEC) provides a wide range of technical and enterprise systems engineering support to the DoD and the intelligence community (IC) at large (The MITRE Corporation, 2012).

The NSA, or the Central Security Service (CSS), roles and responsibilities are charter by Executive Order 12333 (National Security Agency [NSA] Central Security Service, 2013). The NSA's mission is to provide an assessment indication for the United States and its allies through signals intelligence (SIGINT) and information assurance (IA) reports and packages that empower computer network operations (CNO). Specifically, the IA mission is to prevent foreign adversaries from obtaining access to sensitive or classified national security information (NSA Central Security Service, 2013).

B. SURVEY FOUNDATION

The development of the data collection plan is approached through a mixed method methodology to be executed consecutively in five phases. Both open-ended and closed-ended questions are utilized. The data collection instrument is based on the validating quantitative data model variant of the traditional concurrent triangulation design type (Creswell & Clark, 2006). The qualitative questions on the electronic survey are supplementary to the quantitative questions. The qualitative questions are expected to provide insight and thought-provoking quotes that can be used to endorse and elaborate the quantitative survey findings (Creswell et al., 2006, p. 65).

Open-ended questions are intended to provide respondents with an opportunity to reply in their own words (Glasgow, 2005). Open-ended questions provide an opportunity to discover ideas that may not be addressed in the survey and to gather respondents' perceptions regarding ways to overcome or address challenges. The researchers are also able to engage with respondents whom have great knowledge and experience in MDM and can provide course-of-action alternatives for the business environment.

The closed-ended questions consist of three variations: closed-ended question with unordered choices, closed-ended questions with ordered choices, and partial closed-ended question (Glasgow, 2005). The use numbers of closed-ended questions with unordered choices are minimal. They focus on the collection of demographic data. The survey instrument utilizes two closed-ended questions with ordered choices. The researchers opted to utilize partial closed-ended, Likert-style questions with a five-point scalar selection with an optional comment or remark section. A Likert-type scalar format is used to measure the respondents' beliefs and attitudes in reference to the following topics: knowledge, functional requirements, and operating model. Specific Likert scales addressing the frequency and evaluation for specific questions are described in following sections.

The five phases are as follows. Phase one consists of the execution of an electronic survey that collects quantitative and qualitative data. The researchers do not expect to capture an extensive qualitative data set through the execution of the electronic

survey. Phase 1a consists of a convenience sample of key informant interviews utilizing the in-depth questionnaire of the data collection instrument. These questions are expected to produce an extensive qualitative data set. Phase two consists of the analysis of the data. The researchers utilized Microsoft Excel to conduct the analysis of quantitative data, which is discussed in the following chapter. Phase three consists of compiling the qualitative and quantitative data results in a logical manner. Phase four is corroborating the quantitative data with the qualitative results. Phase five is the holistic interpretation of the problem set utilizing the combination of quantitative and qualitative data (see Figure 11).

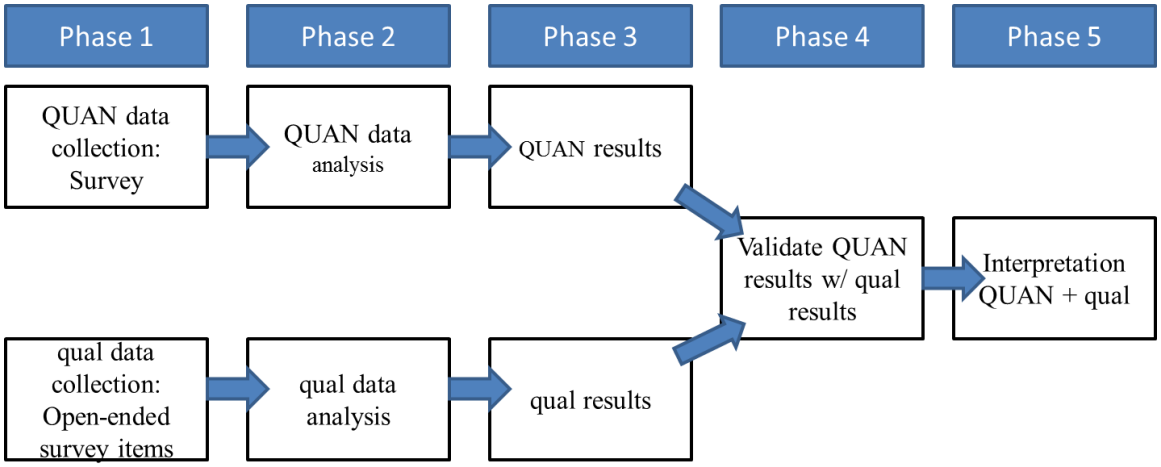


Figure 11. Triangulation Design: Validating Quantitative Data Model (After Creswell & Clark, 2006, p. 63)

C. SURVEY INSTRUMENT

Within the federal government, several organizations have conducted commercial market research in reference to MDM releasing requests for information (RFIs) for sourcing solutions. The researchers draw heavily from a request for information (RFI) released by the Department of the Army, Army Contracting Command, Program Manager Network and Enterprise Services (PM NES), and the DoD *Technology Readiness Assessment (TRA) Deskbook* (Director, Research Directorate, Office of the Director, Defense Research and Engineering [DRD DDR&E], 2009) in formulating the survey instrument.

The instrument layout is logically separated into three distinct parts preceded by an introductory page. Part one focuses on the collection of respondents' demographic data. Part two focuses on capturing information on MDM functional requirements. Part three is intended as an avenue for respondents to provide additional input on topics identified in Part two or expound into areas not addressed in Part two.

The survey instrument was created using the online survey tool Survey Monkey (see Appendix I). The execution of an electronic survey will allow for the greatest number of respondents at the lowest cost. Additionally, an electronic survey allows for the filtering of respondents, which can be accomplished by a method that is commonly referred to as "piping," or the act of directing specific questions to respondents though the application of question logic associated to the respondents' answers during the execution of the electronic survey.

1. Introduction Page

The introduction page, commonly referred to as a welcome screen, is lengthy. For that reason, it is separate from the first question. The researchers incorporate the topics that Sue and Ritter (2012, p.60) suggest that a welcome screen should: "describe or reiterate the purpose of the survey, explain how the respondent was selected for participation, discuss the conditions of anonymity and confidentiality…" The researchers followed the advice of Sue and Ritter (2012) and designed the survey instrument to be motivational, easy to respond to, and contain instructions guiding respondents through the course of the survey.

2. Demographics

The demographics section, question one thru seven, of the survey consists of close-ended questions that request respondents to make a self-assessment. Respondents are asked a series of questions in order to capture general demographic information. This section is intended to serve two purposes. The first is to capture a baseline snapshot of knowledge, experience, and qualifications of the target population. This baseline can be used to address validity and reliability concerns surrounding respondents' answers. The second purpose is to allow for cross-tabular analysis between demographic groups.

The previously mentioned organizations deal directly with the planning, implementation, and technical evaluation of IT networks and hardware. For this reason, the amount of individuals with MDM knowledge and experience within these organizations should be adequate for a convenience sample. The following general duty titles are specified in the survey instrument: network administrator (NA), system administrator (SA), information assurance security manager (IASM), information assurance security officer (IASO), cryptologist (Crypto), chief information officer (CIO), chief technology officer (CTO), designated approval authority (DAA), and select personnel included in the Defense Acquisition Workforce Improvement Act (DAWIA; 1990). See Appendix G for a detailed listing of career fields, related duties, position titles, and a crosswalk of civilian personnel codes to their uniformed service equivalences.

Question one is presented as a multiple-choice, "select-one" format. Respondents are asked to "pick the best option that describes you." The response options are: uniformed service, federal civilian, or DoD contractor. This question acts as piping question. If the respondent selects uniformed service, they are directed to questions two and three. If the respondent selects federal civilian, they are required to answer question four. Those respondents that select DoD contractor are not part of the target population (see the section titled Qualification/Disqualification).

Question two is presented in a multiple-choice, select-one format with selections arrayed in two vertical columns. Respondents are asked to select their Service component. The response options are: Army, Air Force, Navy, Marines, and Coast Guard. Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

Question three is presented in a multiple-choice, select-one format with selections arrayed in three vertical columns. Respondents are asked to "specify your pay grade." The response options are: O1, O2, O3, O4, O5, O6, O7, O8, O9, O10, WO1, WO2, WO3, WO4, WO5, E1, E2, E3, E4, E5, E6, E7, E8, and E9. Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

Question four is presented in a multiple-choice select one format with selections arrayed in two vertical columns. Respondents are asked to select their pay grade. The response options are: GS1, GS2, GS3, GS4, GS5, GS6, GS7, GS8, GS9, GS10, GS11, GS12, GS13, GS14, GS15, SESI, SESII, SESIII, SESIV, and SESV. Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

Question five is presented in a multiple-choice, select-one format with selections arrayed in three vertical columns. Respondents are asked to "select your Agency/Organization/Unit." The response options are: DISA, DHS, NIST, CERDEC, MITRE, RDECOM, and NSA. Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

Question six is presented in a multiple-choice, select-one format with selections arrayed in one horizontal row. Respondents are asked to "pick the best option that describes you." The response options are: information technology professional (i.e., SA [system administrator], NA [network administrator], SME [subject matter expert]), acquisition professional (i.e., KO [contracting officer], PM [program manager], 2210 [information technology management series], information assurance (i.e., IASM [information assurance security manager], IASO [information assurance security officer], Crypto), and information technology manager (i.e., CIO [chief information officer], CTO [chief technology officer], DAA [designated approval authority]). Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

Question seven is presented in a multiple-choice, select-one format with selections arrayed in three vertical columns. Respondents are asked to select "your primary DAWIA certification." The response options are: contracting, information technology, life cycle logistics, PQM [program quality management], program management, SPRDE-PSE [Systems Planning, Research, Development and Engineering-Program Systems Engineer], SPRDE S & TM [Systems Planning, Research, Development and Engineering - Science and Technology Management], SPRDE-SE [Systems Planning, Research, Development and Engineering- Systems Engineering], and

test and evaluation. Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

3. MDM Target Knowledge

The target knowledge section of the survey instrument is primarily structured to confirm the target population's understanding of MDM and, secondarily, to filter out respondents who should not be included in the research.

Question eight is presented in a multiple-choice, select-one format with selections arrayed in one horizontal row. Of note, this question is one of two closed-ended questions with ordered choices utilized in the survey. Respondents are asked if they "have sufficient product experience/knowledge in order to contribute to the expansion of DoD's knowledge in regards to Mobile Device Management?" Response options are *yes* or *no*. This is intended as a piping question to allow respondents to proceed to Part two – functional requirements. If *no* is selected, respondents are not considered part of the target population and are directed to the disqualification page (see the section titled Qualification/Disqualification).

Question nine is presented in a multiple-choice, select-one format with selections arrayed in one horizontal row. Respondents are asked "To what extent does your unit/agency/organization provide training to IT/AC/IS professionals on MDM?" Response options are: To a large extent, To a moderate extent, To some extent, To little extent, and Not at all. Following in the style of the partial closed-ended questions, a "comment/remarks" block is provided for qualitative input.

Question 10 is presented in a multiple-choice, select-all-that-apply format with selections arrayed in two vertical columns. Respondents are asked, "What type of training do you require to become proficient in MDM?" Response options are: iOS and Android operations systems, types of material solution, cost benefit analysis, information security, and bring your own device (BYOD). Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

4. Qualification/Disqualification

The target population is based on a convenience sample of the total population of which there are two disqualifiers. The first possibility for disqualification is determined by the role of the respondent, as addressed in question one. If the respondent selects DoD contractor, that respondent is piped to the disqualification notification for reasons previously outlined. The second reason for disqualification is based on the respondents' perceived knowledge of MDM. Question eight requires the respondent to respond to a closed-ended question with a yes or no, acknowledging whether they possess sufficient product experience/knowledge to contribute to the expansion of the DoD's knowledge in regards to MDM. If respondents answers *no* to this question, they are piped to a disqualification notification page.

5. Part 2—Functional Requirements

The functional requirements are addressed in questions 11 through 22. Respondents are asked to identify the importance of individual attributes of the functional requirements using a partial closed-ended question with Likert-type, five-point scalar selections and an optional comment or remark section. Each question utilizes the same five-point scalar selection of very important, somewhat important, neither important nor unimportant, somewhat unimportant, and very unimportant. The optional comment or remark section is there to provide the respondent an opportunity to respond to any of the questions or concepts presented in the survey (Glasgow, 2005).

The researchers draw on functional requirements as defined by the Army RFI from Army Contracting Command (2011), identified as follows:

- Software distribution is defined as the ability to manage and support mobile application use including deploy, install, update, delete, or block.
- Policy management is defined as the development, control, and operations of DoD enterprise mobile access, connectivity, and security policy.
- Inventory management is defined as the software, firmware, hardware, and peripheral device inventory management; this includes provisioning and support.

- Security management is defined as the implementation and enforcement of DoD-level device security, authentication, validation, and encryption functionality.

Questions 11, 12, and 13 address the policy management function. Respondents are asked, "How important are the following attributes for policy management to MDM?" The data is collected over a series of three questions for ease of the respondent. Data is presented in the confines of one screen, thereby eliminating the need to scroll up or down. The question is presented in a multiple-choice, select-one format as a table with the defining attributes of policy management arrayed in the left-most vertical column. Attributes include the following: administer policies as groups, administer policies as individuals, complex password enforcement (strong alphanumeric password), enable browser enforcement through DoD proxy, enforce URL and web content filtering, support complex group policies (multilayered, hierarchical, etc.) and/or individual policies, support granular restrictive access to specific public app repositories and/or specific applications on specific public app repositories, alert system for users and IT administrators when device policies are violated, which includes the ability to "kill" devices when they become noncompliant, enforce DoD logon banner or custom text to device lock, force exclusive use of VPN for all Internet protocol (IP) traffic, policy compliance reporting, query for compliance and security information, restrict access to enterprise servers, administrator/remote reset of device password, CAC/PIV [common access card/personal identification verification] device authentication, device lock (after a given period of inactivity), disable automatic connection to Wi-Fi networks, disable infrared (IR) port, disable Wi-Fi radio, remote device lock, and remote device wipe (both selective and total).

Questions 14 and 15 address the security management function. Respondents are asked, "How important are the following attributes for security management to MDM?" The data is collected over a series of two questions for ease of the respondent. Data is presented in the confines of one screen, thereby eliminating the need to scroll up or down. The question is presented in a multiple-choice, select-one format as a table with the defining attributes of security management arrayed in the leftmost vertical column. Attributes include the following: bluetooth profile whitelist/blacklist by peripheral type,

bluetooth profile whitelist/blacklist by vendor, disable bluetooth radio, disable camera(s), disable cellular radio, disable microphone(s), disable removable media port, disable access to public app repositories (i.e., App Store, Android Market, etc.), disable location based services (GPS), disable screen capture, disable USB [Universal Serial Bus]/serial port (i.e., 30 pin dock connector, microUSB, miniUSB, etc.), disable use of preinstalled browser, disable voice dialing, and support restrictive management of USB/serial access by vendor and/or peripheral type.

Question 16 addresses the inventory management function. Respondents are asked "How important are the following attributes of inventory management to MDM?" The question is presented in a multiple-choice, select-one format as a table with the defining attributes of inventory management arrayed in the leftmost vertical column. Attributes include the following: device activation and deactivation; device configuration and imaging; enforce mobile communication expense policies, such as disabling cellular data or access to servers when roaming internationally; query support for device and network information; and trouble ticket and tracking management.

Question 17 addresses the software distribution function. Respondents are asked, "How important are the following attributes of software distribution to MDM?" The question is presented in a multiple-choice, select-one format as a table with the defining attributes of software distribution arrayed in the leftmost vertical column. Attributes include the following: access to private application repository, backup/restore of configuration data, backup/restore of software, push and/or pull over-the-air (OTA) software updates for applications and operating systems (OSs), and trusted controls for over-the-air (OTA) or tethered provisioning and updating process.

Question 18 addresses the malware control management in reference to MDM. Respondents are asked, "How important are the following attributes of malware control management to MDM?" The question s presented in a multiple-choice, select-one format as a table with the defining attributes of malware control management arrayed in the leftmost vertical column. Attributes included antivirus and malware detection, phishing protection, and spam protection.

Question 19 addresses e-mail in reference to MDM. Respondents are asked, "How important are the following attributes of e-mail to MDM?" The question is presented in a multiple-choice, select-one format as a table with the defining attributes of e-mail arrayed in the leftmost vertical column. Attributes included CAC/PIV encryption and signing integration, DoD global address list (GAL) integration, integrated calendaring, plain text only native e-mail enforcement, and S/MIME [Secure/Multipurpose Internet Mail Extension] capability.

Question 20 addresses VPN management in reference to MDM. Respondents are asked, "How important are the following attributes of VPN management to MDM?" The question is presented in a multiple-choice, select-one format as a table with the defining attributes of VPN management arrayed in the leftmost vertical column. Attributes include: CAC/PIV encryption and signing integration, DoD global address list (GAL) integration, integrated calendaring, plain text only native e-mail enforcement, and S/MIME capability.

Question 21 addresses administration and reporting tools in reference to MDM. Respondents are asked, "How important are the following attributes of administration and reporting tools to MDM?" The question is presented in a multiple-choice, select-one format as a table with the defining attributes of administration and reporting tools arrayed in the leftmost vertical column. Attributes include the following: a certificate of networthiness (CoN); access to management server via single or web based console role based access, business intelligence, analytics, and reporting tools; enterprise platform integration (i.e., LDAP, Blackberry enterprise server, sood mobile messaging, certificate authority, trouble ticketing and help desk, such as Remedy); FIPS 1402 level 1 encryption of administrative (MDM) communications; group based action management; and integration of hard and/or soft token user authentication (i.e., common access card [CAC], microSD, near field communication (NFC), etc.).

Question 22 addresses rating the functional requirements in reference to MDM. Respondents are asked, "How important to you are the following functions to MDM?" The question is presented in a multiple-choice, select-one format as a table with the defining functions of MDM arrayed in the leftmost vertical column. The functions

include the following: administration and reporting tools, e-mail, inventory management, malware control management, policy management, security management, software distribution, and VPN management.

6. Operating Model

Ross et al. (2006a) define an operating model as follows: the necessary level of business process integration and standardization for delivering goods and services to customers. In the case of MDM, goods and services are defined in general terms as telecom and data applications. Customers are the end users of these goods and services. For this research, the customers are uniformed service members and federal civilians.

Question 23 is presented in a multiple-choice, select-one format with selections arrayed in a vertical column. Respondents are asked, "What best describes your organizations operating model?" Response options are: replication, diversification, coordination, and unification. Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

Question 24 is presented in a multiple-choice, select-one format with selections arrayed in one horizontal row. Respondents are asked, "How dependent is your unit/agency/organization transactions dependent on the availability, accuracy, and timeliness of other units/agencies/organizations data?" Response options are as follows: not very dependent, somewhat dependent, dependent, very dependent, and extremely dependent. Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

Question 25 is presented in a multiple-choice, select-one format with selections arrayed in one horizontal row. Respondents are asked, "How beneficial to your unit/agency/organization is it for your individual units/agencies/organizations to run their operations in the same way?" Response options are as follows: not very beneficial, somewhat beneficial, beneficial, very beneficial, and extremely beneficial. Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

7. Technology Readiness Level

The National Aeronautics and Space Administration (NASA) established the practice of Technology Readiness Levels (TRLs) in the 1980s in order to describe the development of individual technology components within various systems. The TRL concept does not certify design validity or indicate what resources are required to advance to higher TRLs. TRLs are an assessment based at a specific time. TRLs play an integral part in the critical technology element (CTE) concept discussed in the following section (DRD DDR&E, 2009). The levels scale from the beginning phases of controlled research (Level 1) to the effective utilization in an assembly (Level 9; see Appendix H).

Question 26 utilizes a partial closed-ended question presented in a multiple-choice, select-one format with selections arrayed in one vertical column. Respondents are provided an opportunity to review the definitions prior to responding to Question 26. Data is presented in the confines of one screen, using an abbreviated version of the TRL definitions, thereby eliminating the need to scroll up or down. Respondents are asked, "What TRL most accurately describes MDM systems?" Response options are: 1) basic principles observed and reported, 2) technology concept and/or application formulate, 3) analytic and experimental critical function and/or characteristic proof of concept, 4) component and/or breadboard validation in laboratory environment, 5) component and/or breadboard validation in relevant environment, 6) system/subsystem model or prototype demonstration in a relevant environment, 7) system prototype demonstration in an operational environment, 8) actual system completed and qualified through test and demonstration, and 9) actual system proven through successful mission operations (DRD DDR&E, 2009). Following in the style of the partial closed-ended questions, an "other (please specify)" block is provided for qualitative input.

8. Part 3—In-Depth Questions

Part three referred to as the in-depth questionnaire, the collection of qualitative data and consists of questions 27 through 55. This part is sub-divided into two sections: the operational experience questionnaire and CTEs. This transition contains a page break that highlights the shift in focus. Respondents are encouraged to provide as much or as

little information as they choose, allowing the opportunity to expound on concepts or issues not addressed previously. The presentation of the survey questions are presented differently than in the previous sections. These questions are presented simultaneously so that the respondents may select which questions to answer and in what order to respond.

Question 27 is a piping question that uses a closed-ended question with unordered choices (yes or no type) presented in a multiple-choice, select-one format arrayed in one horizontal row. This question is one of two closed-ended questions with ordered choices utilized in the survey. Respondents are asked if they "Have experience in the deployment, integration, management and/or operational usage, of a MDM system?" Response options are yes or no. This is intended as a piping question to allow respondents access to the operational experience portion of the in-depth questionnaire. If the respondents answer with yes, confirming that they have experience in the deployment, integration, management, and/or operational usage of a MDM system, they are directed to questions 28 to 37. If the respondents answer with no, they are directed to questions 38 to 55, the CTE portion of the in-depth questionnaire.

a. Operational Experience

Questions 28 to 37 are open-ended questions crafted to gather respondents' thoughts on tactics, techniques, and procedures (TTPs); systematic issues or concerns; operational capabilities; operational strengths/weakness; and/or any other operational considerations. The data collection effort attempts to gather input from respondents through questions crafted to link system capabilities to an operational capability which has impacted the unit/agency/organization (M. Kalainoff, personal communication, August 2010).

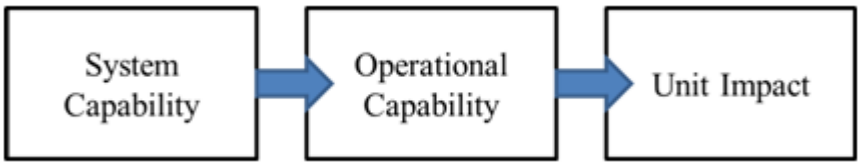


Figure 12. Linking System Capability to Operational Capability With Unit Impact (After M. Kalainoff, personal communication, August 2010)

b. Critical Technology Elements

Questions 33 to 55 are open-ended questions modeled after the DoD *Technology Readiness Assessment (TRA) Deskbook*, intended to gather qualitative data in reference to CTEs (DRD DDR&E, 2009). CTEs can be hardware or software. The *TRA Deskbook* defines a CTE as follows: a technology element is "critical" if the system being acquired depends on this technology element to meet operational requirements (within acceptable cost and schedule limits), and if the technology element or its application is either new, or novel, or in an area that poses major technological risk during detailed design or demonstration. Specific questions in the areas of system design, commercial use, terminal hardware, processing hardware, networking hardware, and scalability are posed.

D. SURVEY DESIGN/IMPLEMENTATION RECOMMENDATIONS SUMMARY

The Defense Acquisition System is built upon phases punctuated by milestones or decision points (DAU, 2012). Porter et al. (2009) identified that defense acquisition executives (DAEs) are reluctant, for cultural reasons, to modify the acquisition program baseline (APB). In addition, Dillard and Ford (2009, p. 249) highlighted that "PMs should understand the nature of their product requirements with regard to their range of attainment and relative to key parameters of capability and vis-à-vis the readiness level of their enabling technologies."

Tomorrow's acquisition programs will not be solely judged on fulfilling the requirements as outlined in the Joint Capabilities Integration Development System (JCIDS). Weapons systems and automated information systems will be assessed against capabilities that the current commercial marketplace can provide. The survey captures input from a broad range of SMEs in order to obtain the product requirement links to operational capabilities with supporting CTEs. In today's uncertain environment, DAEs could utilize this survey and its subsequent data, as outlined in Chapter V, to dynamically align program investments while focusing on affordability.

V. EXAMPLE RESULTS, INTERPRETATION, AND RECOMMENDATIONS FOR FUTURE RESEARCH

A. SAMPLE DATA GENERATION

The researchers chose to generate random results for the survey using Microsoft Excel. Only questions one through 26 of the survey are used in the artificially generated dataset (see Appendix J). Questions 27 through 55 are not addressed in this section because they contain short-answer questions that are qualitative in nature.

The possible responses for questions one through 26 are each assigned a whole, sequential numerical value according to the number of responses in each question. Question two asks the respondents to select their Service. The possible selections include: Army, Air Force, Navy, Marines, and Coast Guard. Therefore, question two is coded as follows: Army (1), Air Force (2), Navy (3), Marines (4), and Coast Guard (5).

The population sample size is 100 respondents. Every respondent has a unique ID of one to 100. The individual respondents follow the logical flow of questions in the survey based on their responses. A majority of the questions are answered by all respondents, but three are dependent on responses to previous questions. Consequently, the number of responses to questions three, four, and seven are less than 100. The dependency questions, and their associated questions and answers, are as follows:

- 3. Please specify your pay grade. Which depends on question one; Pick the best option that describes you. (Response: uniformed service)
- 4. Please specify your pay grade. Which depends on question one; Pick the best option that describes you. (Response: federal civilian)
- 7. What is your primary DAWIA certification? Which depends on question six; Please pick the best option that describes you. (Response: acquisition professional)

Two exclusionary responses exist within the survey that disqualify the respondent from proceeding with the survey. The researchers have excluded these responses from the example. The questions that could cause respondents to be disqualified from the survey, and the answers that would disqualify them, are as follows:

- Question one. Pick the best option that describes you. (Response: DoD contractor)
- Question eight. Do you believe that you have sufficient product experience/knowledge in order to contribute to the expansion of DoD's knowledge in regards to Mobile Device Management? (Response: no)

For each question, the researchers performed functions in Microsoft Excel that randomly chose a number within the range of possible responses. For most of the questions, the =RANDBETWEEN([lower], [upper]) function was used to generate a random whole number between a lower and upper bound. For question two, this function looked like this: =RANDBETWEEN(1,5). The response to this function was a randomly generated whole number between one and five.

As noted previously, question two is dependent on a response from question one. To perform this calculation, the researchers used the function =IF([logic_test], [value_if_true], [value_if_false]). This assigned a specified value to the function if certain designated criteria were met. For question two, this looked like this: =IF([Question one's Cell] = 1,1,0). With a response of uniformed service (1) to question one, the IF function in question two resulted in a value of one; any other response resulted in a value of zero.

Putting an IF and RANDBETWEEN statement together in the same function allowed for the effective generation of a random response to questions that were dependent on another question's response. For question two, this looked like this: =IF([Question one's Cell] = 1,1,0)*RANDBETWEEN(1,5). This function multiplied the randomly generated number by one if uniform service(1) was chosen as a response to question one, resulting in a randomly generated number between one and five for question two. If uniform service was not chosen as a response to question one, the randomly generated number was multiplied by zero, resulting in a null amount for question two.

Appendix C contains the aggregate response rates for each survey question. Copies of the detailed data records are maintained with the primary investigator. Individuals may contact the primary investigator for request procedures.

B. RESULTS AND INTERPRETATION

The following sections walk through the results of the random response data to the survey questions, utilizing cross tabulation and graphical display techniques found in Microsoft Excel. The results are to demonstrate the possibilities for interpretation of the data generated from the survey questions. The results do not encompass all of the possibilities for interpretation of the data. They are examples of the scope and level of detail that the data can provide.

1. Demographic and Target Knowledge Results

Part one of the survey, questions one through 10, covers demographics and target knowledge. The responses to part one capture a great deal of information and provide a snapshot of who participated in the survey. The survey is intended for federal IT and acquisition professionals with a functional knowledge of MDM. The goal is to have a widely distributed demographic population that encompasses several organizations within the DoD and federal government. The response rate to question one shows a nearly even split between uniformed service members (51) and federal civilians (49) (see Figure 13). With this response rate, the aggregate results of the survey contain a nearly equal distribution of weight from the two groups. When the respondent numbers of one group within a population significantly outnumbers another group, it must be factored in when interpreting the data. Results containing a disproportionate number of respondents from a certain group will likely have results that are skewed towards that group's perspective.

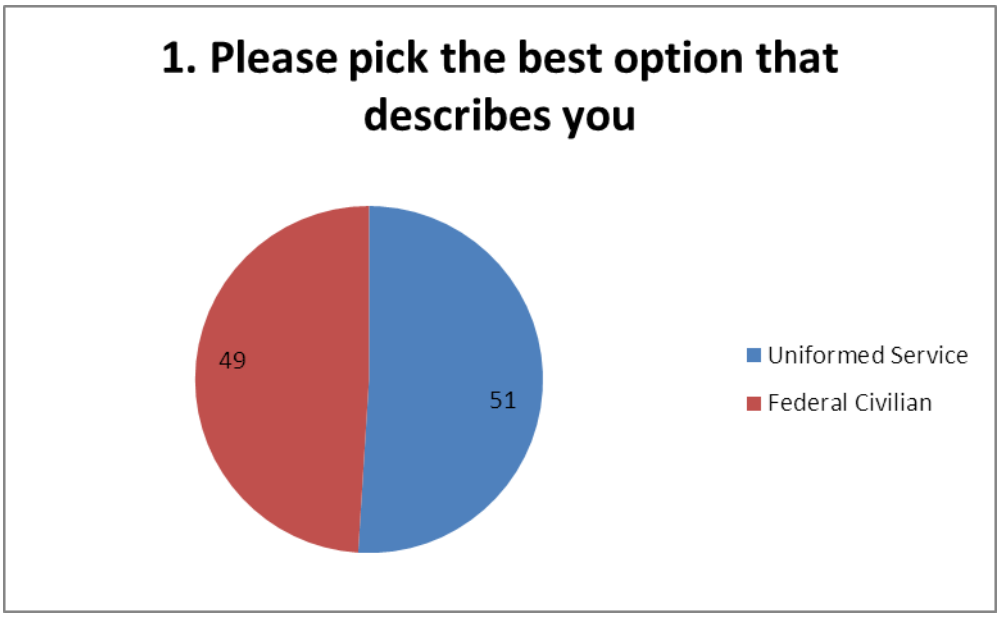


Figure 13. Unformed Service Versus Federal Civilian Response Rate

Within the uniformed service respondents, there is less of an even distribution across the service components. The Marines are the largest response group and represent 27.5 percent of the respondents, followed by the Navy (21.6 percent), Air Force (19.5 percent), Army (15.7 percent), and Coast Guard (15.7 percent). (see Figure 14). Given this data, an assumption can be made that the uniformed service data on the survey is slightly skewed towards the Marine's perspective.

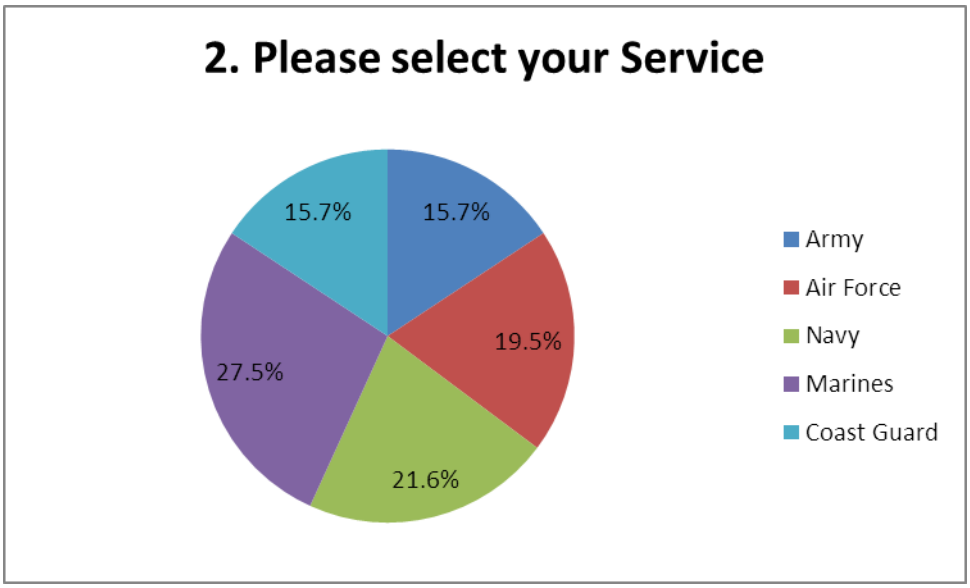


Figure 14. Uniformed Service's Response Rate

The researchers also examined the individual responses of the organizations within the federal civilian demographic and found similar distribution to that of the uniformed service. The largest percentage of respondents is the "other" group at 22.4 percent. This group comes from organizations not individually listed on the survey. With such a high percentage in the other group, it might be worth attempting to determine if there are additional organizations that warrant an individual listing in the survey. The second largest percentage of respondents within the federal civilian demographic are from CERDEC at 18.4 percent, followed by MITRE (14.3 percent), DISA (10.2 percent), NIST (10.2 percent), NSA (10.2 percent), DHS (8.2 percent), and RDECOM (6.1 percent) (see Figure 15). As noted in chapter IV, MITRE is a leader in federal research on MDM, are federally funded, and not-for-profit. For these reasons, the researchers have included them in the federal civilian data source pool.

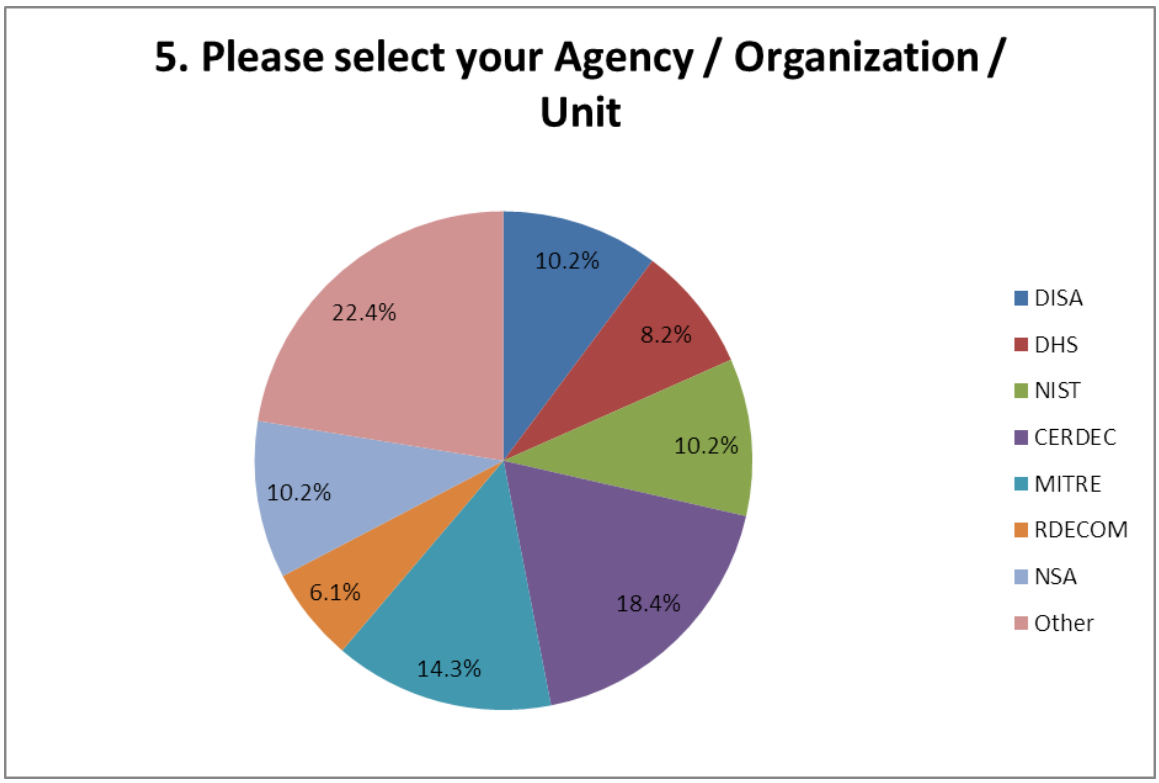


Figure 15. Federal Civilian Response Rate

The researchers are interested in gaining perspective on MDM from both a technical and acquisitions viewpoint. Question six shows that only 19 percent of the respondents described themselves as being acquisitions professionals. ITM professionals made up 23 percent of the respondents, followed by IA (21 percent) and IT professionals (17 percent) (see Figure 16). The researchers anticipate that a majority of the respondents who meet the survey criteria of being proficient in MDM will have a technical professional background. A response rate like this would validate the researcher's assumption, with 61 percent of respondents coming from the technical professional backgrounds of IA, IT, and ITM. In addition, the percentage of technical background respondents may be even higher, depending on the responses received for the "other" group.

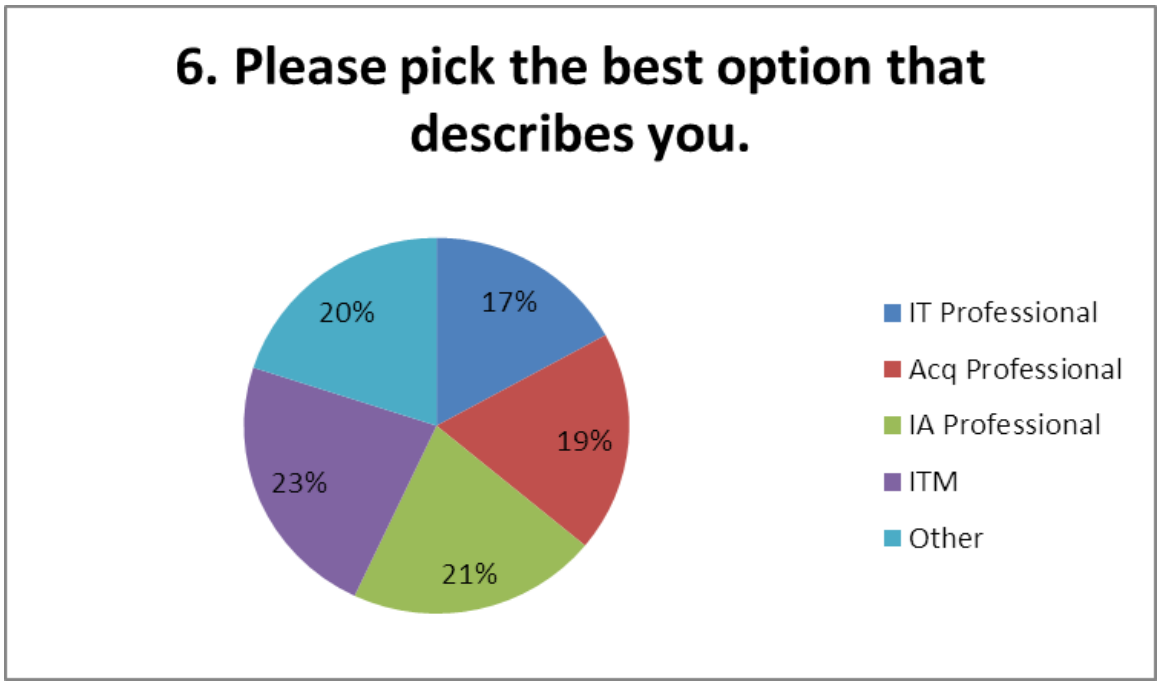


Figure 16. Respondents' Professional Backgrounds

All of the uniformed service and federal civilian respondents to the survey are asked question eight: Do you believe that you have sufficient product experience/knowledge in order to contribute to the expansion of DoD's knowledge in regards to Mobile Device Management? Regardless of their responses, respondents answer questions 9 and 10.

Question 9's average response has a Likert value of 3.11, meaning that the average respondent of the survey feels that their organization provides some level of training on MDM. Cross-tabulating questions 2 and 9 allows for a breakdown of the level of MDM training that each Service branch provides. The data shows that the Air Force has the highest level of MDM training with a Likert average of 3.22; while the Army has the lowest at 2.75 (see Figure 17).

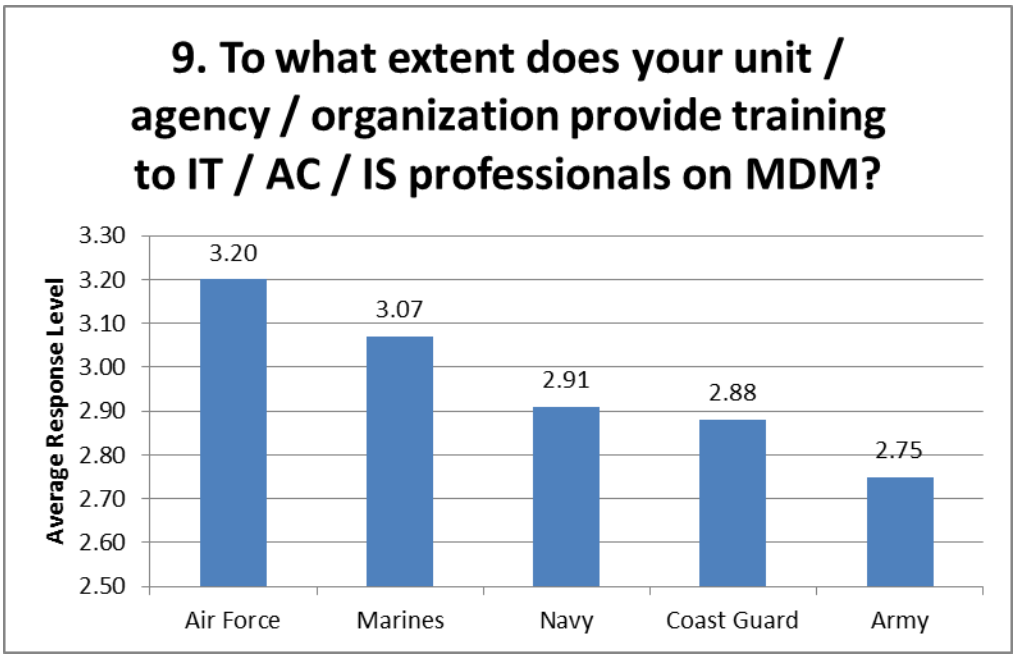


Figure 17. Service Branch MDM Training Level

Cross-tabulating questions five and nine allows for the same type of analysis for the federal civilian organizations. The results of this cross-tabulation show a much wider distribution across the different organizations, with the DHS having the highest average response level of 4.0 and the DISA the lowest at 2.2 (see Figure 18). An average response level of 4.0 means that the DHS provides a moderate level of MDM training. An average response level of 2.2 means that the DISA provides little MDM training.

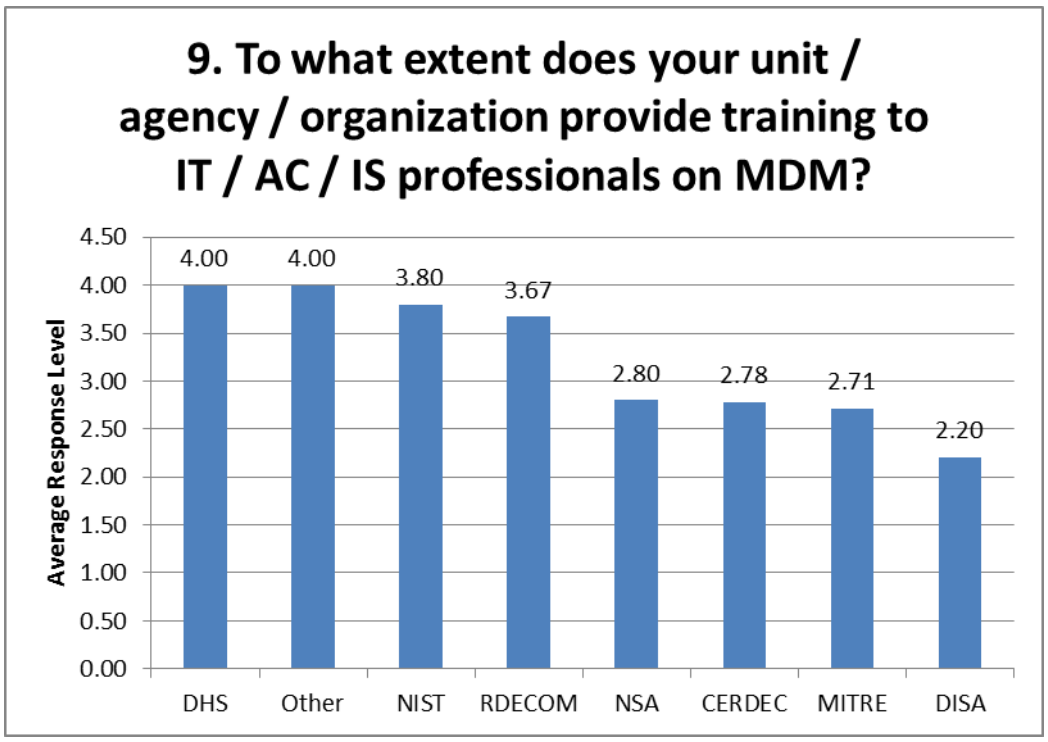


Figure 18. Federal Civilian Organizations' MDM Training Level

Question 10 should show what areas of training the respondents feel are required to become proficient in MDM. The data shows that the respondents feel there are a wide variety of training areas that make an individual proficient in MDM. Over 50 percent of the respondents agree that training in different types of material solutions (53 percent), information security (51 percent), and other areas (50 percent) are required to become proficient in MDM (see Figure 19).

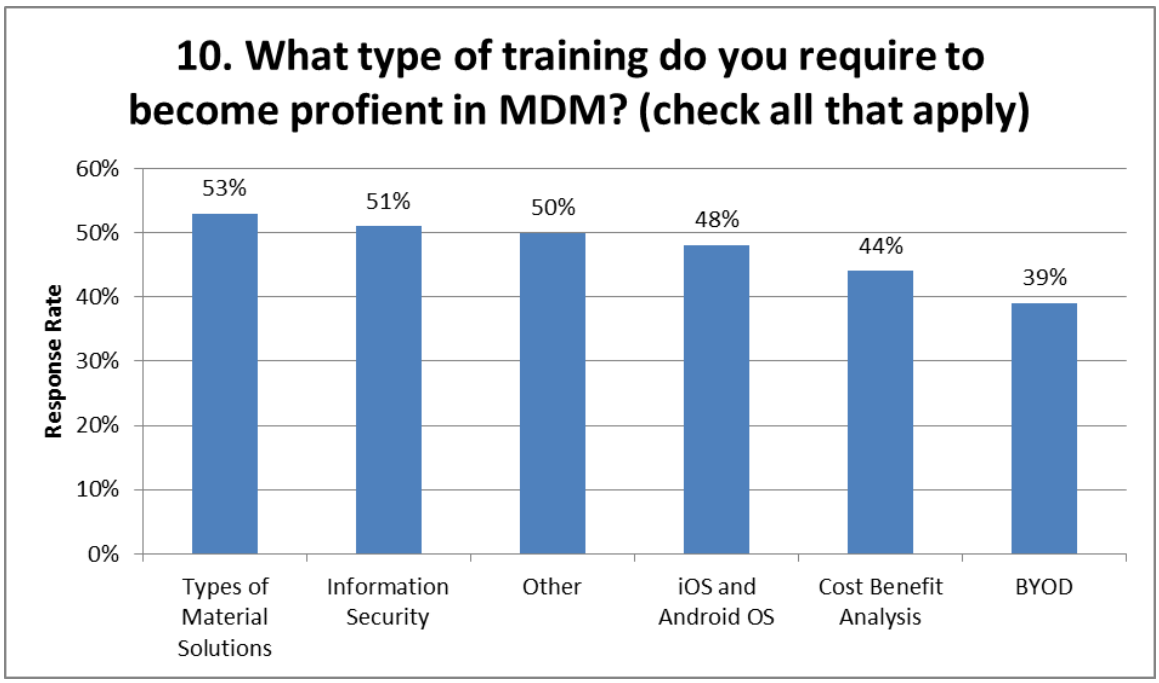


Figure 19. Training Required for Proficiency in MDM

Cross-tabulating questions two and 10 shows what each Service branch believes is needed when training to become proficient in MDM. The data results would indicate that the most important training requirement for any Service branch is training on the types of material solutions to the Navy, with an 82 percent response rate. The least important requirement cited is training on BYOD to the Air Force, with a 10 percent response rate (see Figure 20).

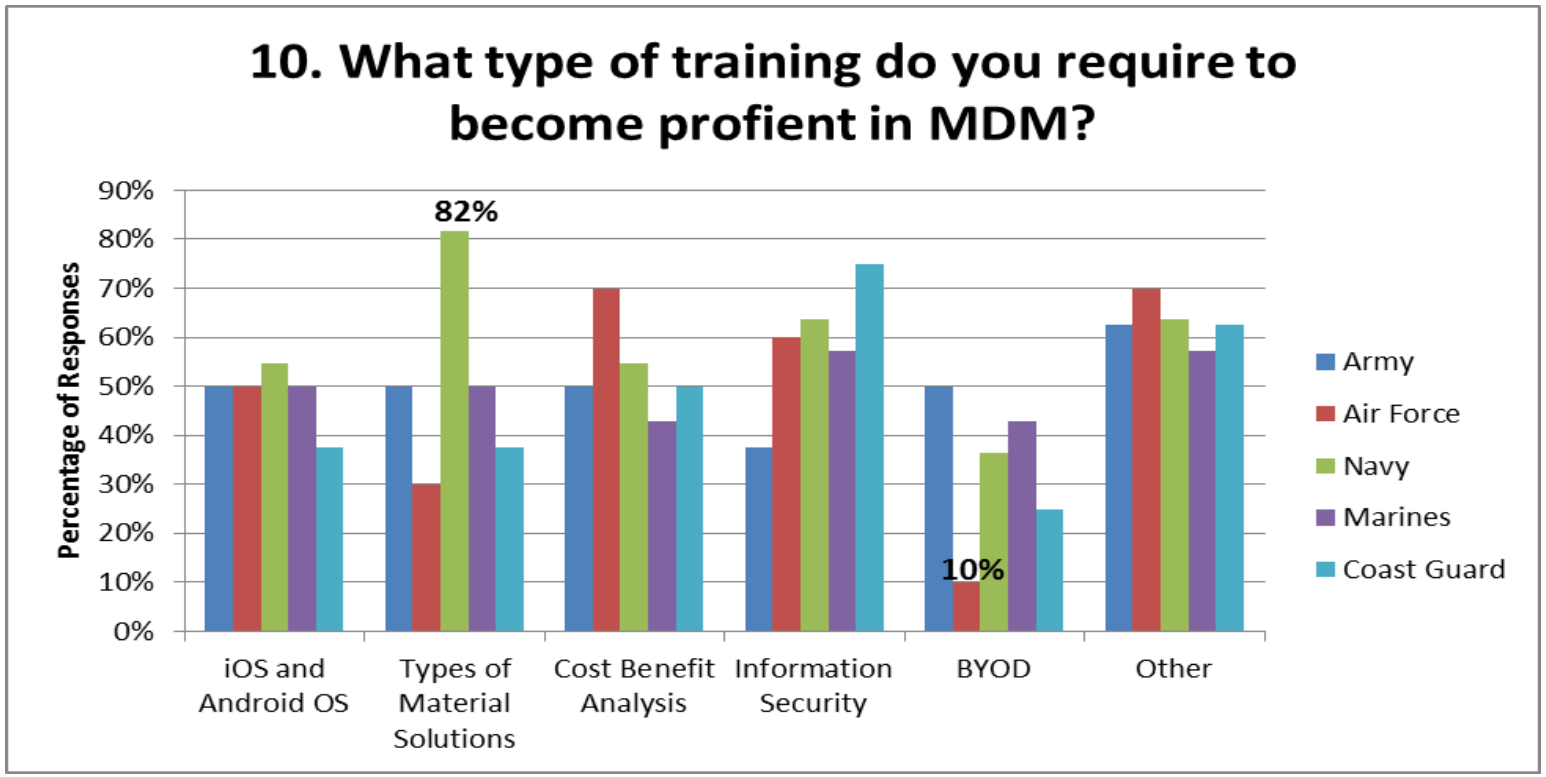


Figure 20. Training Required for Uniformed Service Proficiency in MDM

Cross-tabulating questions five and 10 shows the type of training that each federal civilian organization believes is required to become proficient in MDM. The data shows that there is a much wider variation of responses to question 10 between the federal civilians than between the uniformed service members. Just as in the uniformed services example, the most important training requirement cited by any federal civilian organization is training on the types of material solutions to MITRE, with an 86 percent response rate. The least important is training on iOS and Android operating systems to the DHS, with a zero percent response rate (see Figure 21).

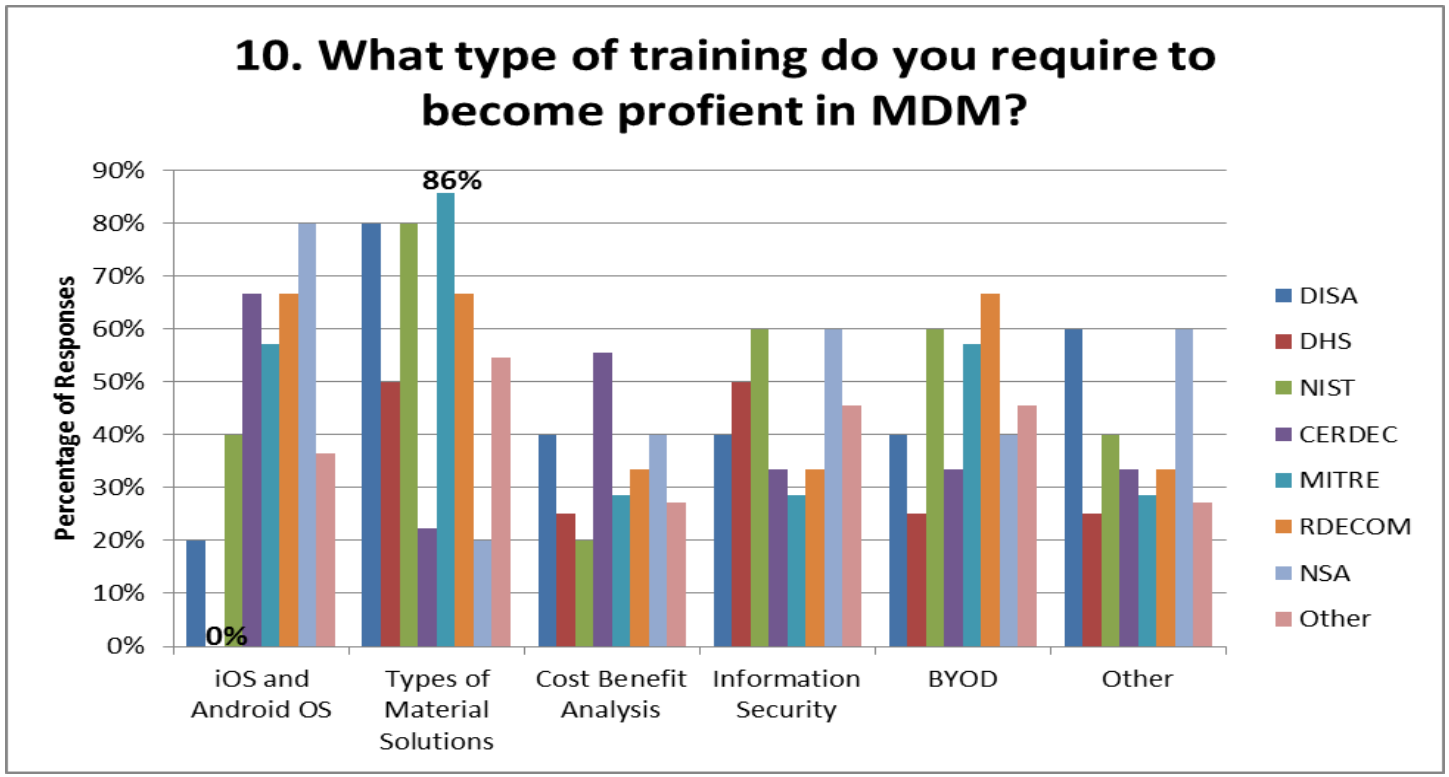


Figure 21. Training Required for Federal Civilian Proficiency in MDM

Cross-tabulating the demographic data from the survey with other section responses allows for the analysis of response rates and level of specific groups and organizations. It is also possible to identify individual responses by cross-tabulating the respondent ID with specific sections or questions. The researchers did not analyze the results on an individual respondent level, but this may be helpful to identify outlier respondents.

2. Outliers and Excluded Responses

Criteria can be set for what constitutes an outlier. For example, if an individual answers the same position on the survey for every question, this pattern of response could be considered a positive indicator of an outlier. The researcher can analyze the outlier responses and determine if they want to include or exclude the associated data.

The disqualifying response to question eight is excluded from the data set. Actual responses to the survey will result in a number of respondents who feel that they do not have sufficient product experience or knowledge in MDM to contribute to the survey. Cross-tabulating disqualifying responses to question eight with question 10 should show what type of training is required to educate more individuals to make them proficient in MDM.

3. Functional Requirements Results

Part two of the survey, questions 11 through 26, captures information on the functional requirements of MDM. Part two contains three sections, which address MDM functions, the operating model, and technology maturity.

a. MDM Attributes

Questions 11 through 22 cover MDM attributes and use the same response profile. Each response corresponds to a Likert value between one and five, as follows:

- Very unimportant—1,
- Somewhat unimportant—2,
- Neither important nor unimportant—3,

- Somewhat important—4, and
- Very important—5.

The Likert values allow for better analysis of the data results through quantification. The attributes with the highest Likert average are those the respondents feel are most important to MDM. The average of the response rate of each attribute within a functional requirement should show the importance of the requirement to MDM.

The data indicates that the most important functional requirements to MDM are security management and inventory management, with an average response level of 3.01. The third most important functional requirement is malware control management at 2.93, followed by e-mail (2.90), administration and reporting tools (2.87), policy management (2.86), VPN management (2.85), and software distribution (2.76; see Figure 22). In the data, the average levels of importance are all within 0.25 points of each other. The researchers expect actual responses to the survey will result in a wider distribution. The results should show what functional requirements to focus on when determining a MDM solution.

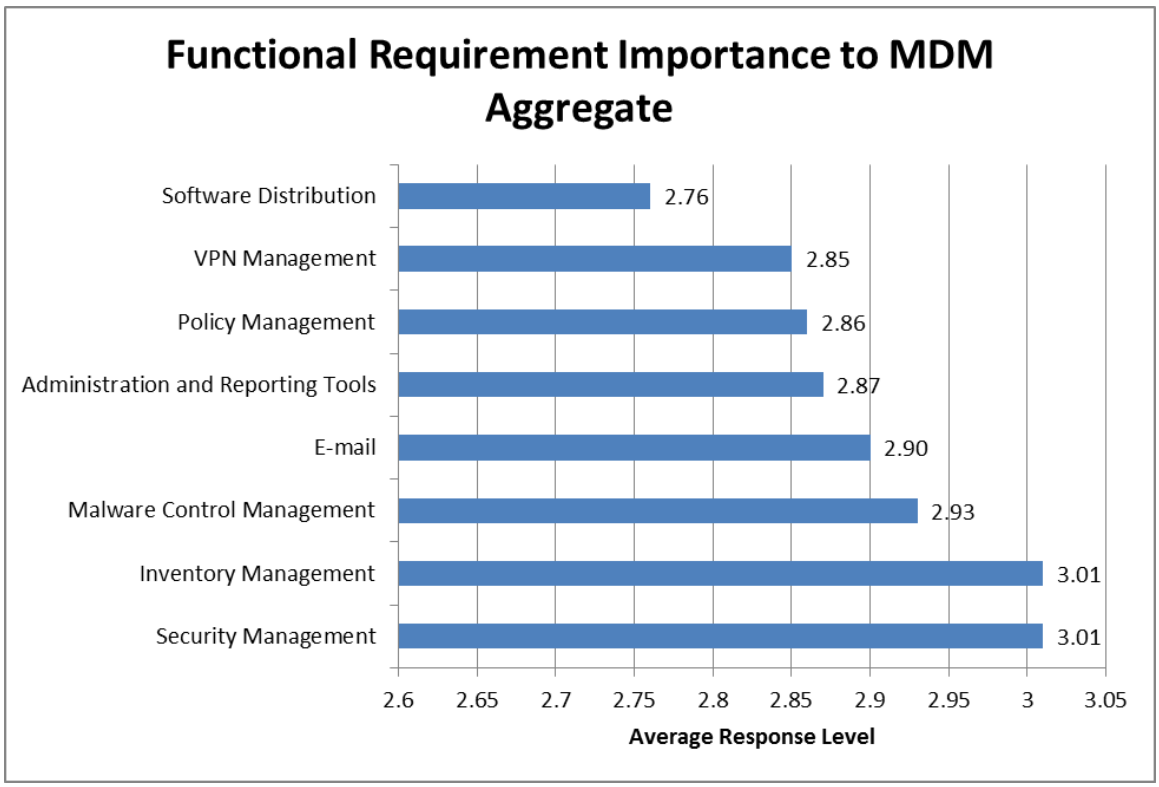


Figure 22. Functional Requirement Importance to MDM

Breaking down the attributes by functional requirement shows what attributes are most important to MDM within the functional requirement. The data shows that within the e-mail functional requirement, integrated calendaring is the most important attribute to MDM at 3.11, while S/MIME capability is least important at 2.78 (see Figure 23).

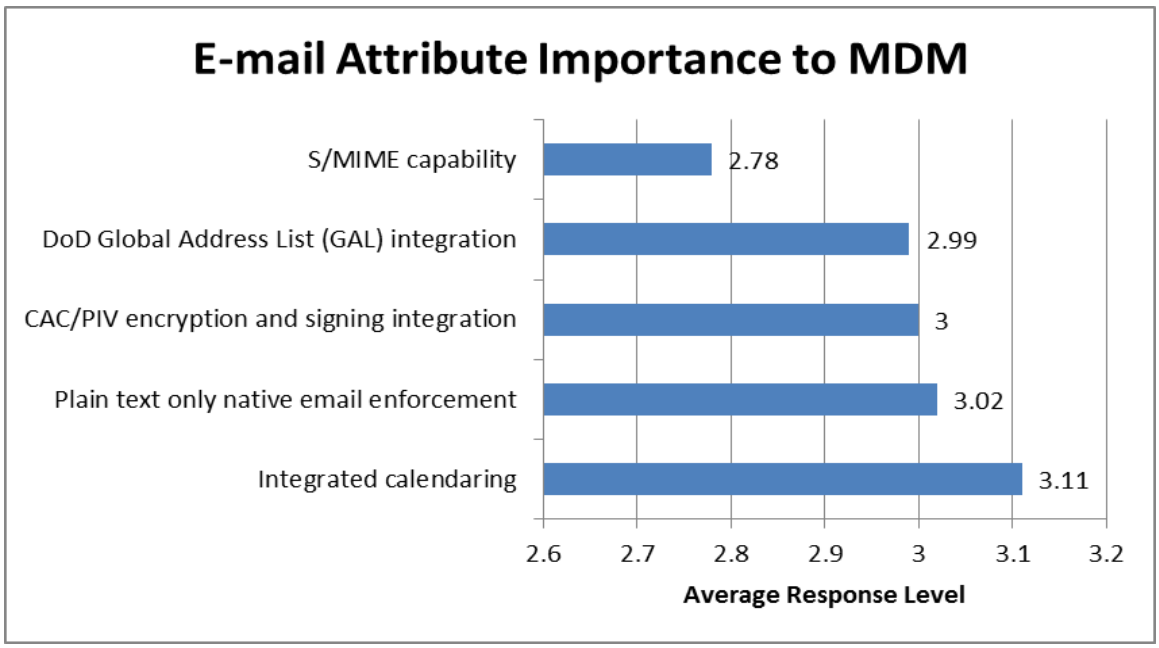


Figure 23. E-mail Attribute Importance to MDM

The data indicates the most important attribute across all of the functional requirements is a certificate of networthiness (CoN) at 3.31. The top 10 most important attributes to MDM are rounded out by the ability to do the following: enforce the DoD logon banner or custom text to device lock (3.22); remote device lock (3.21); disable automatic connection to Wi-Fi networks (3.20); IPSec/SSL end to end encryption (3.18); enforce URL and web content filtering (3.18); PKI based authentication (3.16); query support for device and network information (3.16); alert system for users and IT administrators when device policies are violated (3.15); and bluetooth profile whitelist/blacklist by peripheral type (3.14; see Figure 24). The most important attributes to MDM should show specifically what the respondents want out of an MDM solution.

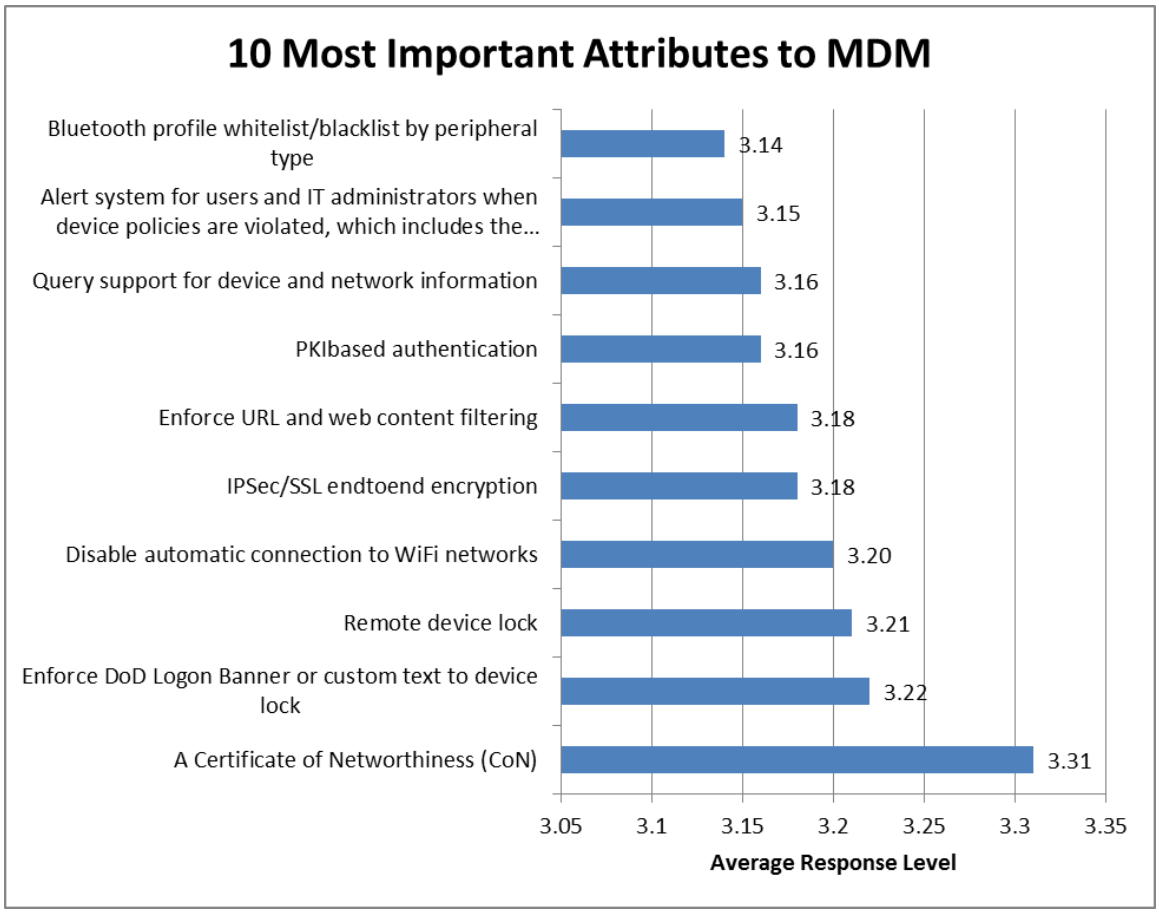


Figure 24. 10 Most Important Attributes to MDM

The least important attributes to MDM start with the ability to query for compliance and security information at 2.57, followed by these attributes: S/MIME capability (2.78); disable use of preinstalled browser (2.78); disable microphone(s) (2.8); enforce mobile communication expense policies, such as disabling cellular data or access to servers when roaming (2.8); disable access to public app repositories (2.82); device activation and deactivation (2.86); phishing protection (2.86); integration of hard and/or soft token user authentication (2.86); disable USB/serial port (2.88; see Figure 25). The attributes with the lowest response levels on the survey might be candidates for elimination from the requirements list.

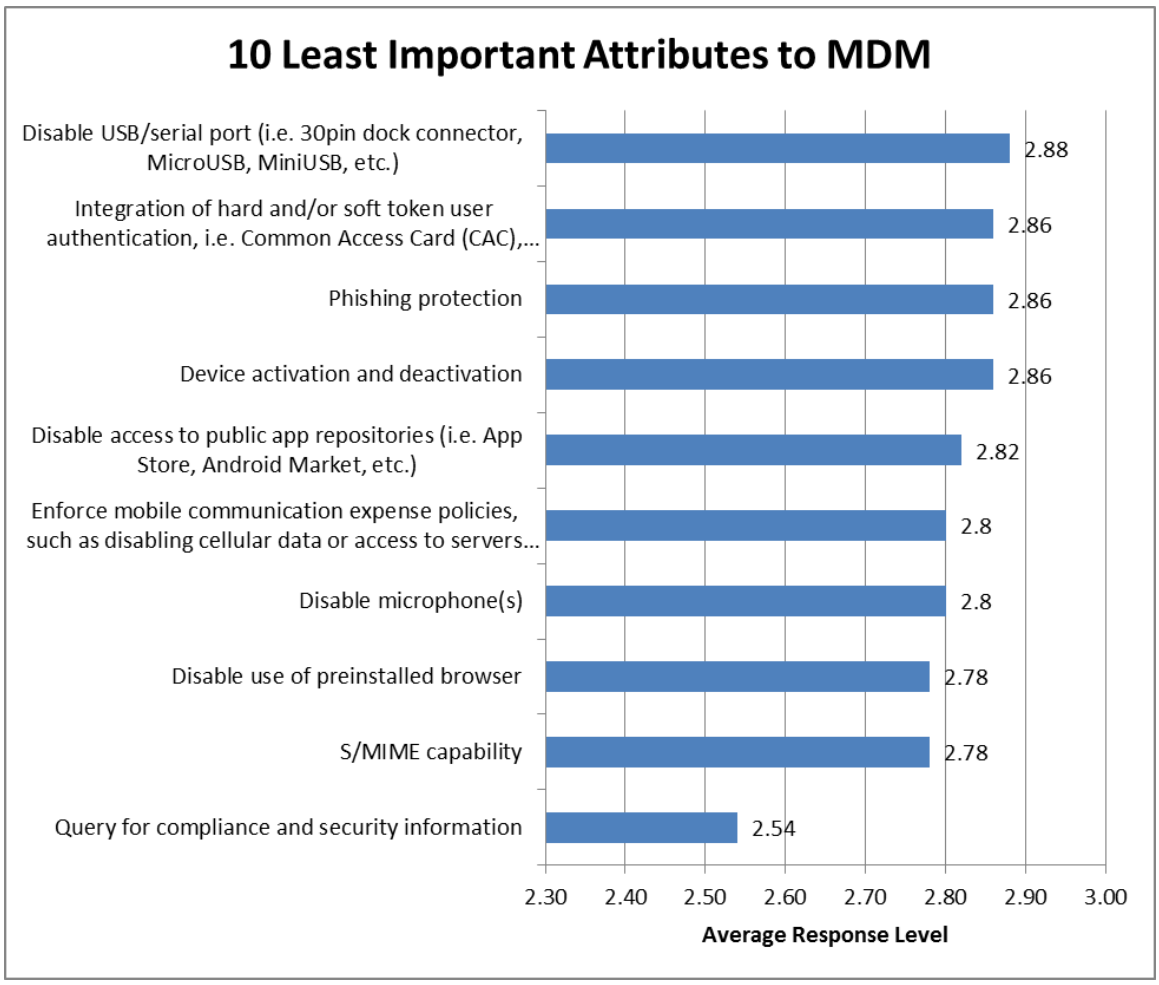


Figure 25. 10 Least Important Attributes to MDM

Questions 11 through 21 ask detailed information about the level of importance of the attributes within each functional requirement. The responses allow for individual attribute levels of importance to MDM. These individual levels factor into the aggregate level of importance for each functional requirement. Question 22 asks the respondents to rate the importance of each functional requirement without looking at the individual attributes. The researchers hope to see similar levels of importance for the functional requirements from the aggregate calculations of questions 11 through 21 and the individual results from question 22. The data does not reflect this. The level of importance assigned to each functional requirement varies noticeably (see Figure 26). Results like this could indicate that some of the individual attributes used for each functional requirement are inaccurate. This would force a reassessment of what attributes

make up each functional requirement. Another possibility could be that a number of individuals within the sample have different understandings of what comprises each functional requirement. The effects of this possibility would diminish through the standardization of terms and definitions and their assimilation into the population.

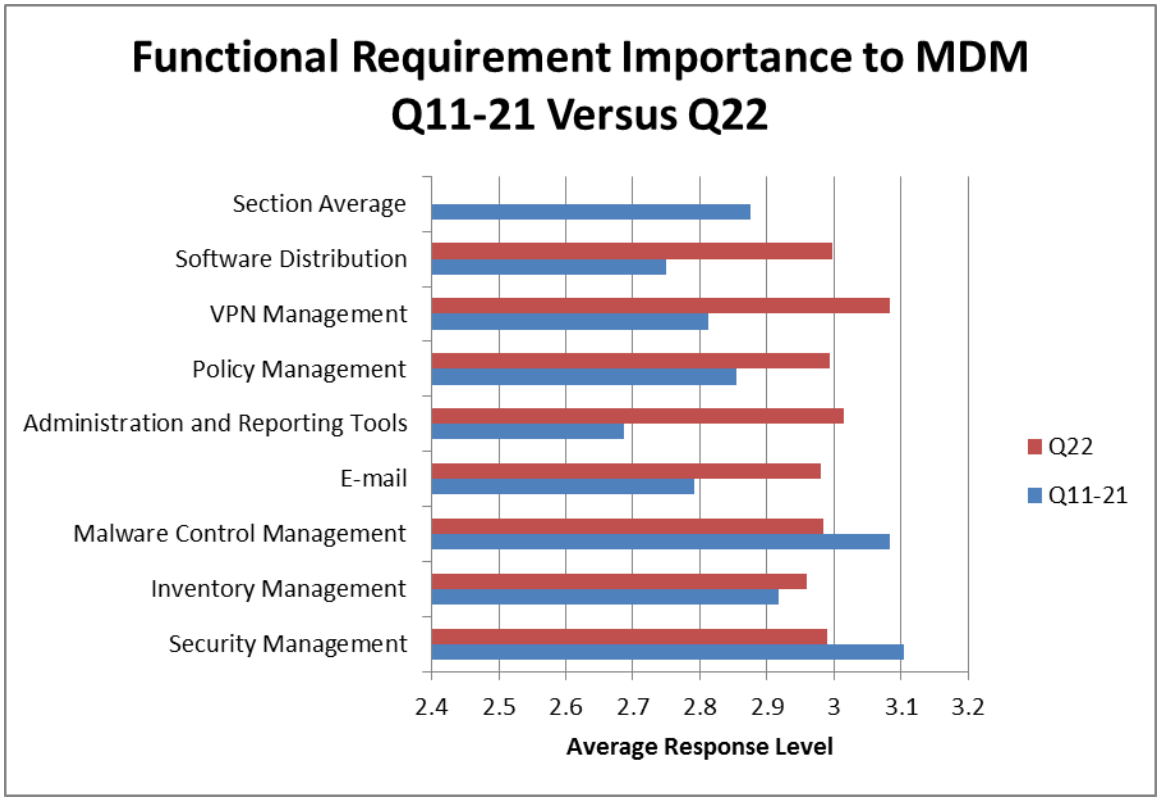


Figure 26. Functional Requirement Importance to MDM Q11–21 Versus Q22

b. The Technology Readiness Level Results

The data for question 26 would indicate that the survey respondents vary on where they feel MDM technological maturity stands. With a 15 percent response rate, most respondents believe that MDM technology is at a TRL of five. Each of the nine TRLs received between a seven and 15 percent response rate (see Figure 27). A higher response rate for the higher TRLs is desired. This would indicate that the respondents feel that MDM technology is mature. Having higher response rates at the lower end of the TRL scale would be cause to reassess whether MDM technology is mature enough to implement.

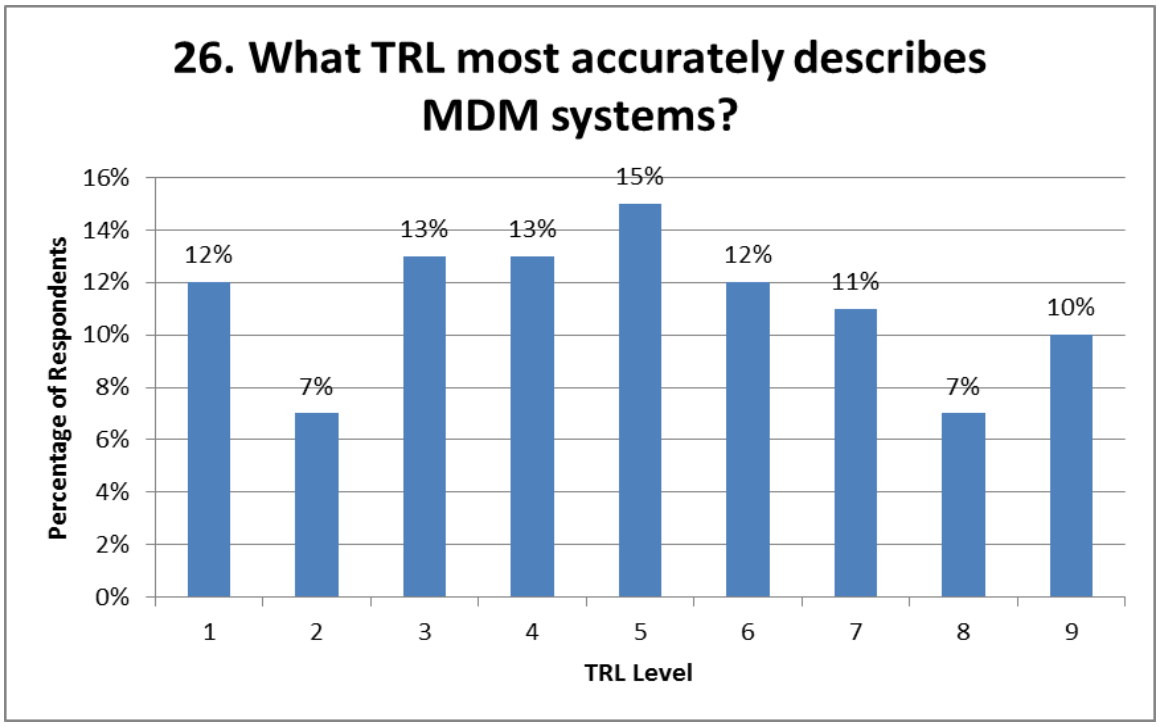


Figure 27. MDM Technology Readiness Level

C. USING THE COST EFFECTIVENESS ANALYSIS MODEL

When using the cost effectiveness analysis model, organizational decision-makers must first determine the relative weights for each of the three evaluation criteria. These weights vary by situation and depend on how important each evaluation criteria is to the given situation. Decision-makers also assign weights to the stakeholder objectives of initial cost and maintenance cost. This allows for greater control over the weights assigned to the purchase price and maintenance costs when evaluating MDM solutions.

The data collected from questions 11 through 21 allows for quantifications of the responses. This, in turn, allows the researchers to feed numbers into the MDM cost effectiveness analysis model. With the data integrated into the model, the next step is to evaluate alternative MDM solutions to determine the optimal choice. The weights of the stakeholder objectives that fall under the CEA model evaluation categories of capabilities and security are calculated with the data from the survey.

The four functional requirements that make up the capabilities evaluation category are inventory management, e-mail, policy management, and software

distribution. These functional requirements are identified under the heading of stakeholder objectives on the cost effectiveness analysis model. To determine the weighted average of the stakeholder objectives under the capabilities category, the individual response levels from the survey are added together and each stakeholder objective is divided by that number. After performing the calculation, inventory management has a weighted average of 0.2611, e-mail has 0.2515, policy management 0.2480, and software distribution 0.2394 (see Figure 28). The same calculations are performed for the stakeholder objectives under the security capability category and result in VPN management with a weighted average of 0.2444, malware control management with 0.2514, security management with 0.2581, and administrative and reporting tools with 0.2461 (see Figure 29).

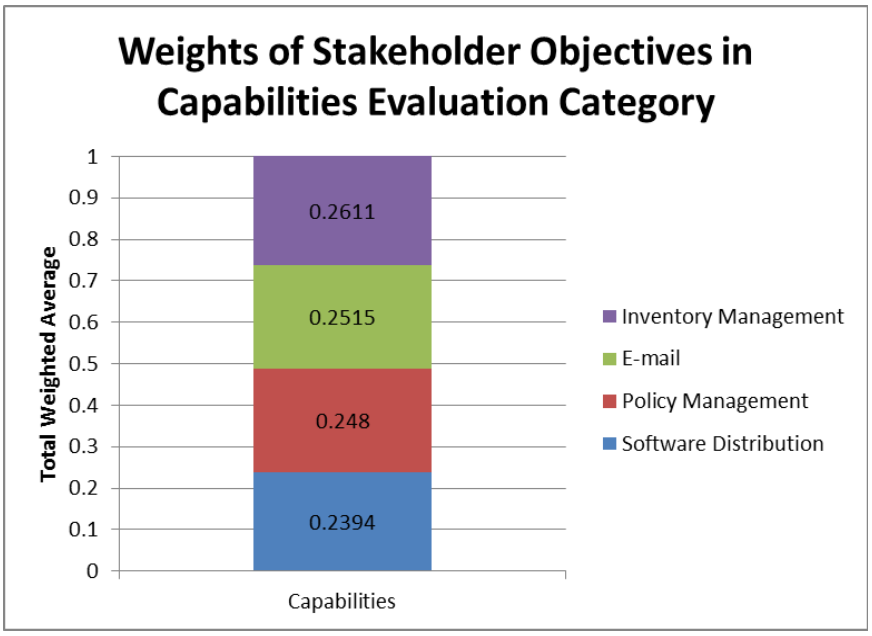


Figure 28. Weights of Stakeholder Objectives in Capabilities Evaluation Category

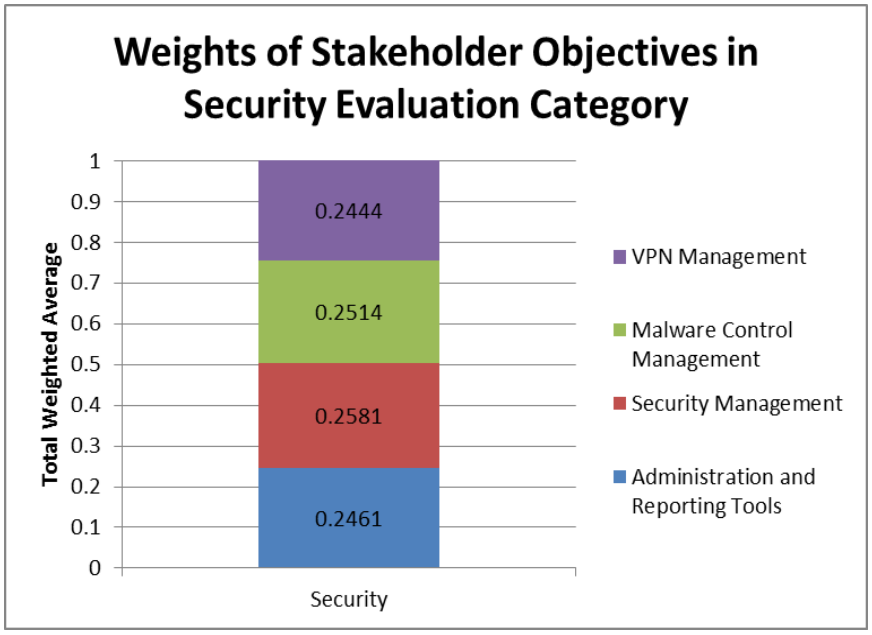


Figure 29. Weights of Stakeholder Objectives in Security Evaluation Category

The attributes listed under each functional requirement in the survey represent the system requirements portion of the MDM cost effectiveness model. Each requirement receives a weight based on its relative importance to MDM under its particular stakeholder objective. A MDM solution either has a system requirement or not. For that reason, the system requirements can be looked at as a checklist when evaluating MDM solutions.

The survey data results in a fairly even assignment of weight values within each stakeholder objective. An example of the even distribution is found within the policy management requirements in which the weight values range from 0.0711 to 0.0885 (see Figure 30). With live data, the dispersion of weights should be more pronounced.

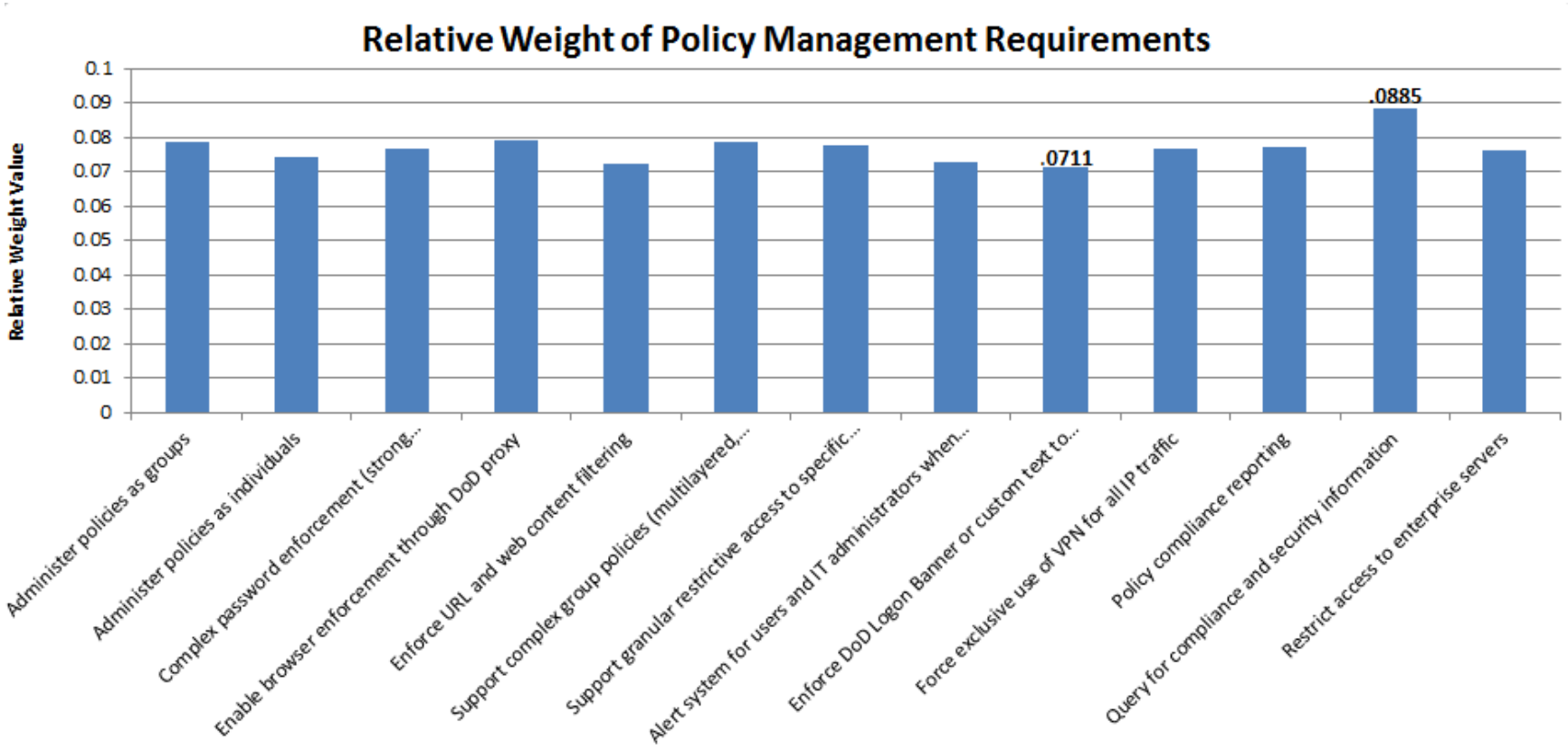


Figure 30. Relative Weight of Policy Management Requirements

D. PRACTICAL APPLICATION OF MDM COST EFFECTIVENESS ANALYSIS MODEL

Next, the researchers constructed a scenario to demonstrate the functionality of the MDM CEA model. The scenario is not modeled after an organization, and the information used is not drawn from any real-life source. The data generated from the survey is used as the basis for the model weights. In this example, the stakeholder objective scores are determined based on the general scenario information. In contrast, when utilizing the model with live information, every MDM solution alternative should be evaluated to determine if it fulfills each individual requirement. The resulting requirements score is then multiplied by its associated stakeholder objective weight to determine the stakeholder objective score.

1. Scenario

Organization A is looking at purchasing a MDM solution. Organization A has formed a special MDM evaluation committee to facilitate the search. The evaluation committee has narrowed the search to three candidates: MDM1, MDM2, and MDM3. The evaluation committee must perform a thorough evaluation on the candidates to determine the optimal MDM solution.

Organization A deals with sensitive information on a regular basis and places high importance on the security of their network and operations. Organization A is looking for a MDM solution with a robust amount of capabilities, but they do not need an all-encompassing solution. Organization A is very profitable, and are willing to pay top dollar for a MDM solution that meets its needs.

MDM1 is a MDM solution designed to address a wide variety of MDM areas. If you can think of it, MDM1 can probably handle it. The initial and maintenance costs of MDM1 are very high.

MDM2 is a MDM solution that takes a more targeted approach to MDM. Its focus is on the security aspects of MDM and has a few other capabilities. The initial and maintenance costs of MDM2 are moderate.

MDM3 has a reputation for value. It offers a modest amount of security and capabilities features. The initial cost of MDM3 is low and the maintenance costs are low/moderate.

2. Assigning Weights

Based on its current situation, Organization A assigns weights of 0.5 to security, 0.3 to capabilities, and 0.2 to TCO. Under the stakeholder objective of TCO, Organization A believes that maintenance cost is of equal importance as the initial cost. The organization assigns a weight of 0.5 to initial cost and 0.5 to maintenance cost (see Figure 31).

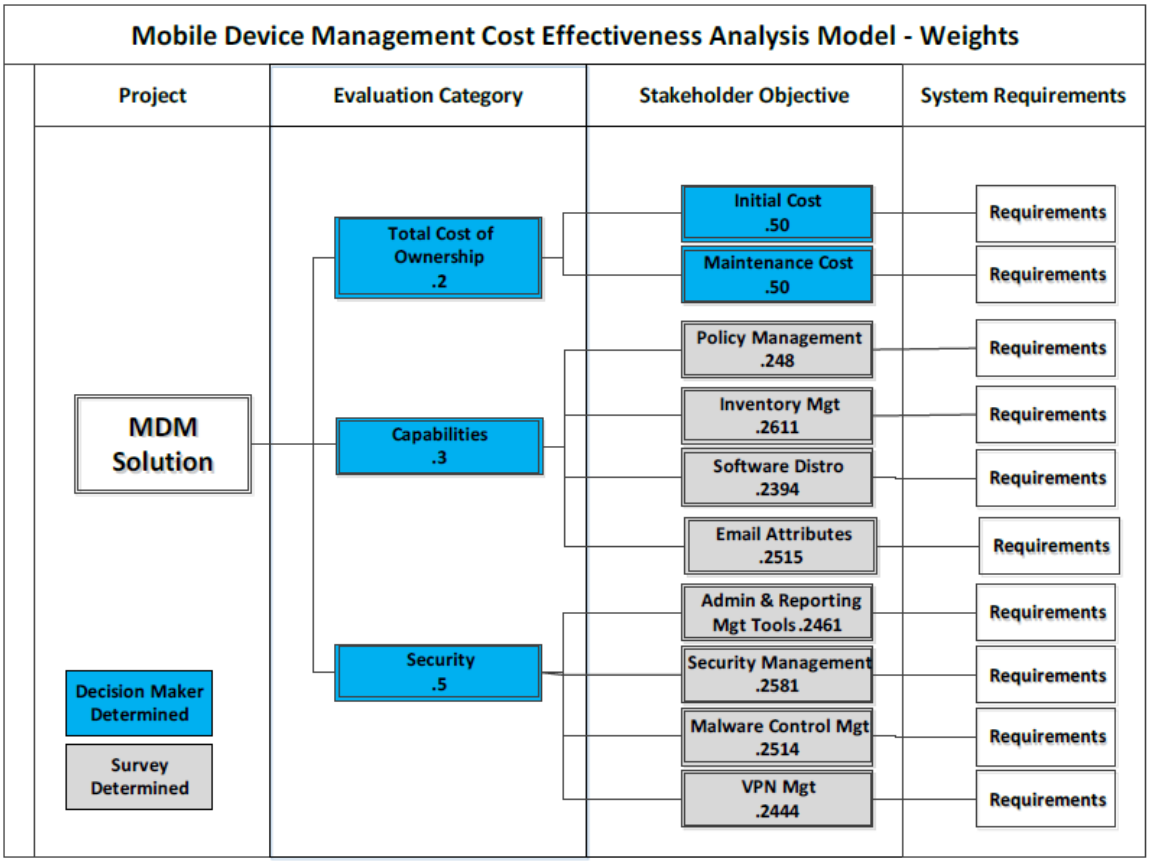


Figure 31. MDM CEA Model, Weights

3. Evaluation of Alternatives

MDM1 receives a TCO, initial cost score of 0.25, and a TCO, maintenance cost score of 0.25. The resulting total TCO score is 0.25. MDM1's total security requirements and total capabilities requirements each score 0.9. Each stakeholder objective score is multiplied by its weight value and added together. MDM1's cost effectiveness score is 0.77 (see Figure 32).

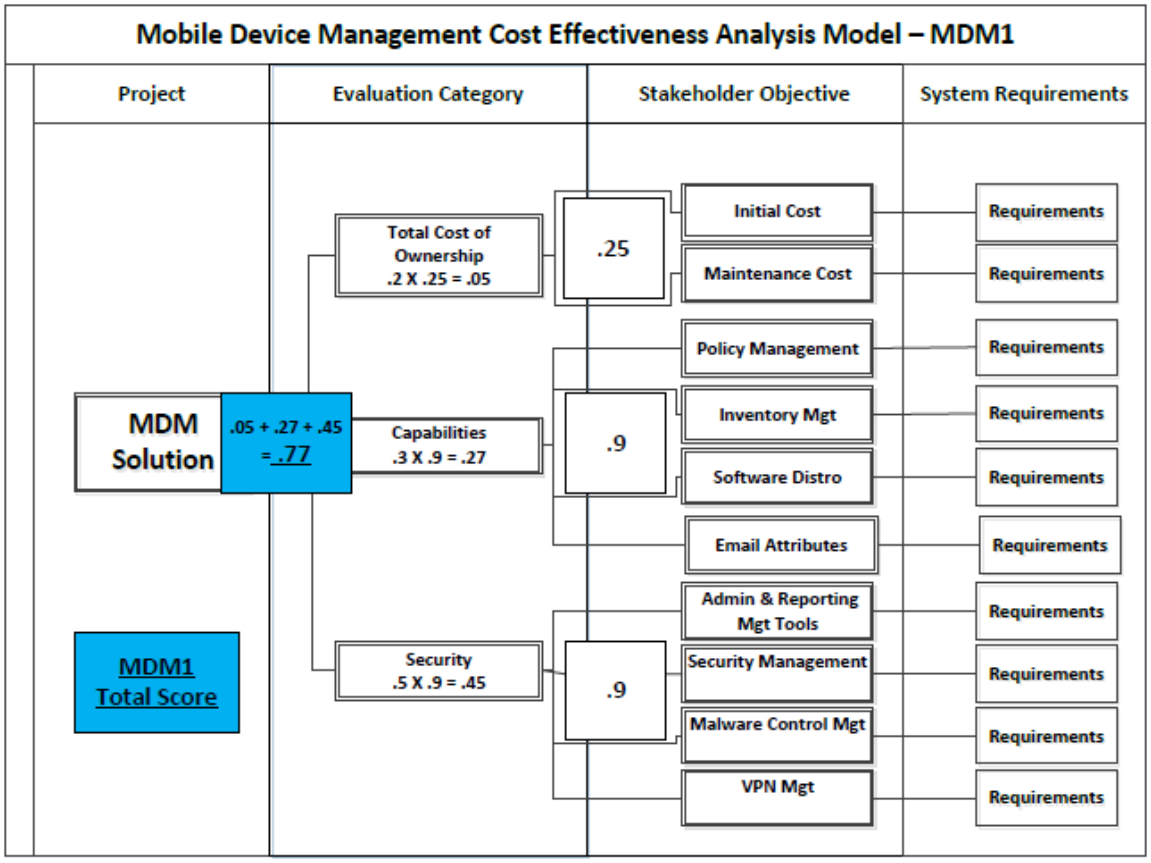


Figure 32. MDM CEA Model—MDM1

MDM2 receives a TCO, initial cost score of 0.5, and a TCO, maintenance cost score of 0.5. The resulting total TCO score is 0.5. MDM2's total security requirements score 1.0 and total capabilities score 0.25. MDM2's cost effectiveness score is 0.675 (see Figure 33).

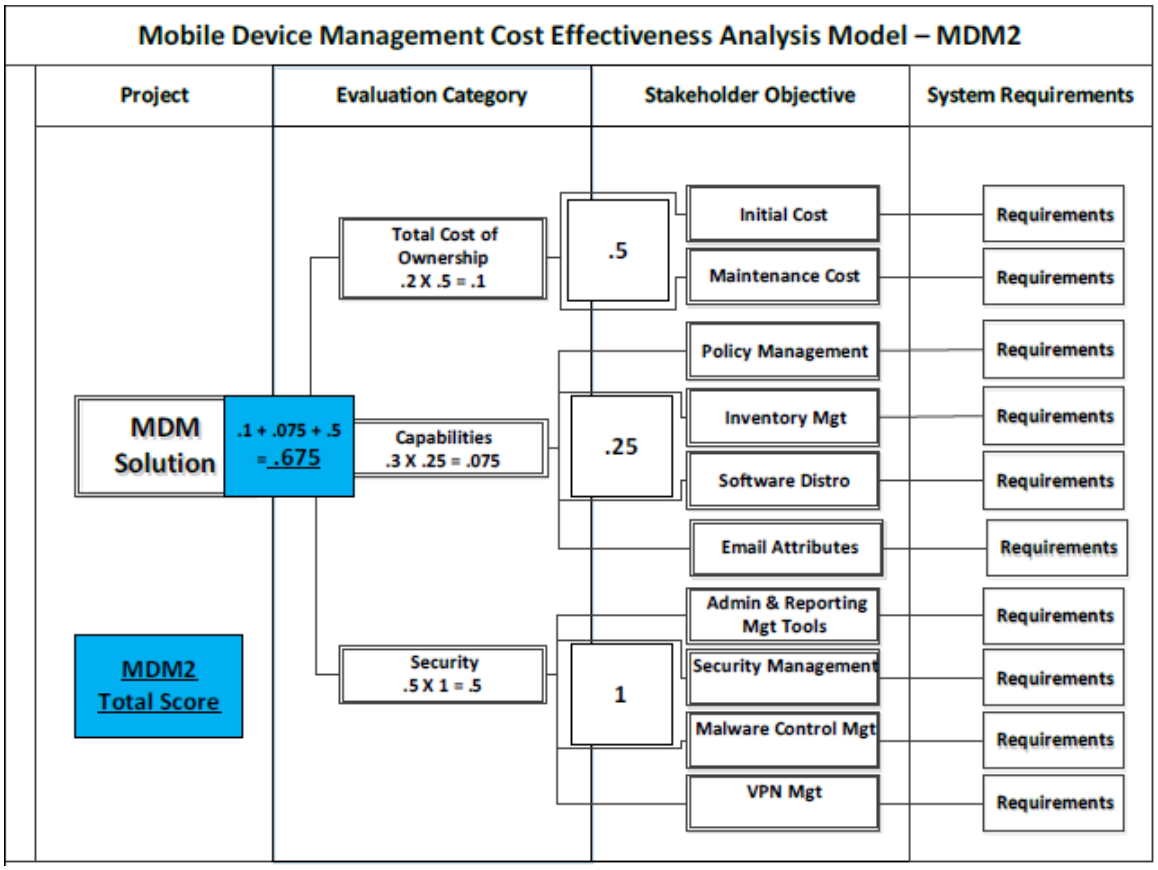


Figure 33. MDM CEA Model—MDM2

MDM3 receives a TCO, initial cost score of 1.0, and a TCO, maintenance cost score of 0.75. The resulting total TCO score is 0.875. MDM3's total security requirements and total capabilities requirements each score 0.5. MDM3's cost effectiveness score is 0.6125 (see Figure 34).

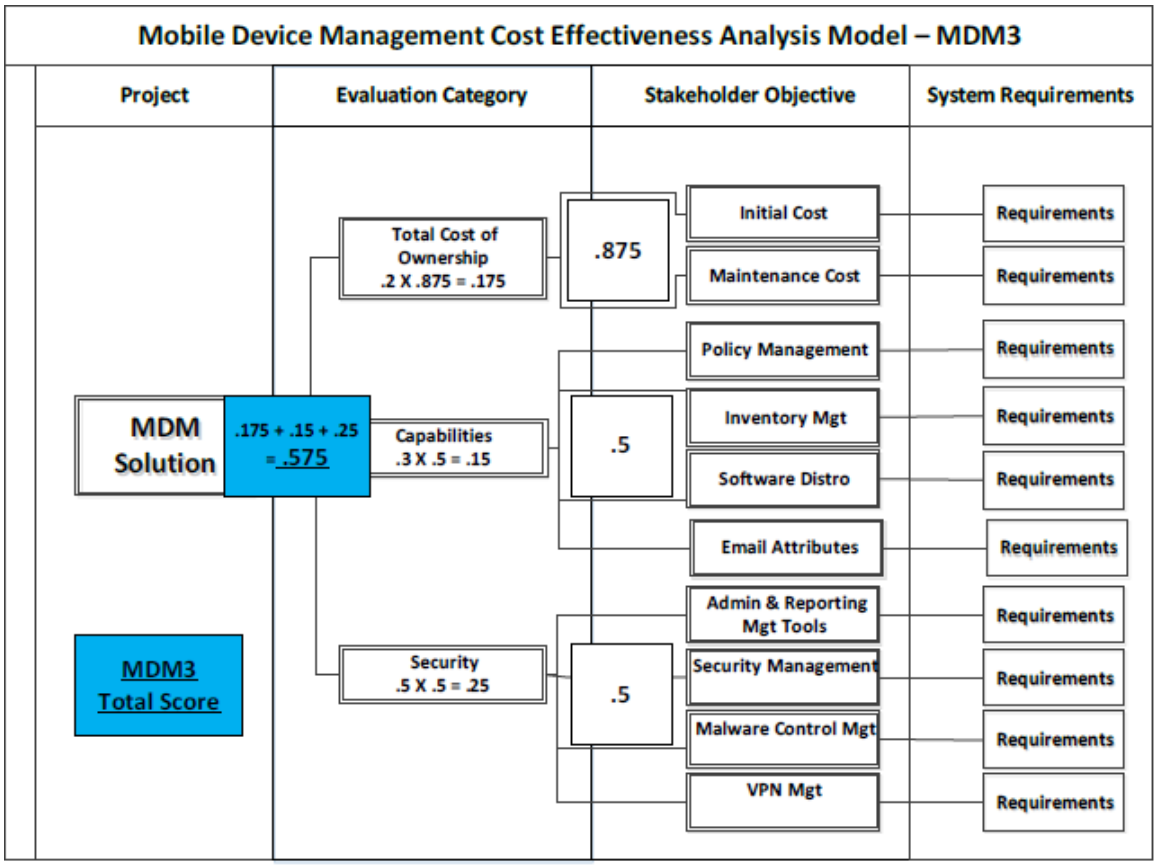


Figure 34. MDM CEA Model – MDM3

MDM1 earns the highest cost effectiveness score, 0.77 out of a possible 1.0. Therefore, MDM1 is the optimal MDM solution for Organization A.

E. RECOMMENDATIONS FOR FUTURE RESEARCH

The top suggestion for future research is the validation and execution of the survey instrument. Validation of the survey should include all of the participating agencies, while the execution must follow all of the applicable regulations governing research on the target population. This includes internal and external organizational oversight such as that provided by an institutional review board (IRB) and the Navy Personnel Research, Studies, and Technology Department (NPRST). A format for a research introduction e-mail is found in Appendix K.

Future research should include the pre-testing of the survey, and could include the execution of focus groups. This would enable the further refinement, modification, and

evaluation of the survey questions while ensuring that the necessary calculations, such as reliability, validity, and Cronbach's alpha, are captured. While this research is focused on the wider scope of the DoD, future research could be focused at a narrower scope, such as at the Service branch level. With slight modifications, this survey tool could be used for MDM research covering a wide variety of sizes and scopes.

The use of automated software tools during the research was minimal. Incorporating decision tree analysis and concept mapping could benefit future researchers through the use of automated qualitative and quantitative research tools. Decision tree analysis could facilitate strategic decision-making through course of action development. Quantitative examples include, but are not limited to, JMP and SPSS. Concept mapping would provide understandable graphical relationships and facilitate coding development for qualitative analysis. Qualitative examples include, but are not limited to, ATLAS.ti, MAXqda, QDA Miner, SMART Ideas, and CMAP.

APPENDIX A. DEFINITIONS OF SOURCES OF MOBILE THREATS

(From GAO, 2012)

Sources of Mobile Threats	
Threat Source	**Description**
Botnet operators	Botnet operators use malware distributed to large numbers of mobile devices and other electronic systems to coordinate remotely controlled attacks on websites and to distribute phishing schemes, spam, and further malware attacks on individual mobile devices.
Cyber criminals	Cyber criminals generally attack mobile devices for monetary gain. They may use spam, phishing, and spyware/malware attacks to gain access to the information stored on a device, which they then use to commit identity theft, online fraud, and computer extortion. In addition, international criminal organizations pose a threat to corporations, government agencies, and other institutions by attacking mobile devices to conduct industrial espionage and large-scale monetary and intellectual property theft.
Foreign governments	Foreign intelligence services may attack mobile devices as part of their information-gathering and espionage activities. Foreign governments may develop information warfare doctrine, programs, and capabilities that could disrupt the supply chain, mobile communications, and economic infrastructure that support homeland security and national defense.
Hackers	Hackers may attack mobile devices to demonstrate their skill or gain prestige in the hacker community. While hacking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and easily launch them against mobile devices.
Terrorists	Terrorists may seek to destroy, incapacitate, or exploit critical infrastructures such as mobile networks, to threaten national security, weaken the U.S. economy, or damage public morale and confidence. Terrorists may also use phishing schemes or spyware/malware to generate funds or gather sensitive information from mobile devices.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. DEFINITIONS OF COMMON MOBILE ATTACKS

(From GAO, 2012)

Common Mobile Attacks	
Attacks	**Description**
Browser exploits	These exploits are designed to take advantage of vulnerabilities in software used to access websites. Visiting certain web pages and/or clicking on certain hyperlinks can trigger browser exploits that install malware or perform other adverse actions on a mobile device.
Data interception	Data interception can occur when an attacker is eavesdropping on communications originating from or being sent to a mobile device. Electronic eavesdropping is possible through various techniques, such as (1) man-in-the-middle attacks, which occur when a mobile device connects to an unsecured Wi-Fi network and an attacker intercepts and alters the communication; and (2) Wi-Fi sniffing, which occurs when data are sent to or from a device over an unsecured (i.e., not encrypted) network connection, allowing an eavesdropper to "listen to" and record the information that is exchanged.
Keystroke logging	This is a type of malware that records keystrokes on mobile devices in order to capture sensitive information, such as credit card numbers. Generally keystroke loggers transmit the information they capture to a cyber-criminal's website or e-mail address.
Malware	Malware is often disguised as a game, patch, utility, or other useful third-party software application. Malware can include spyware (software that is secretly installed to gather information on individuals or organizations without their knowledge), viruses (a program that can copy itself and infect the mobile system without permission or knowledge of the user), and Trojans (a type of malware that disguises itself as or hides itself within a legitimate file). Once installed, malware can initiate a wide range of attacks and spread itself onto other devices. The malicious application can perform a variety of functions, including accessing location information and other sensitive information, gaining read/write access to the user's browsing history, as well as initiating telephone calls, activating the device's microphone or camera to surreptitiously record information, and downloading other malicious applications. Repackaging—the process of modifying a legitimate application to insert malicious code—is one technique that an attacker can

	use.
Unauthorized location tracking	Location tracking allows the whereabouts of registered mobile devices to be known and monitored. While it can be done openly for legitimate purposes, it may also take place surreptitiously. Location data may be obtained through legitimate software applications as well as malware loaded on the user's mobile device.
Network exploits	Network exploits take advantage of software flaws in the system that operates on local (e.g., Bluetooth, Wi-Fi) or cellular networks. Network exploits often can succeed without any user interaction, making them especially dangerous when used to automatically propagate malware. With special tools, attackers can find users on a Wi-Fi network, hijack the users' credentials, and use those credentials to impersonate a user online. Another possible attack, known as bluesnarfing, enables attackers to gain access to contact data by exploiting a software flaw in a Bluetooth-enabled device.
Phishing	Phishing is a scam that frequently uses e-mail or pop-up messages to deceive people into disclosing sensitive information. Internet scammers use e-mail bait to "phish" for passwords and financial information from mobile users and other Internet users.
Spamming	Spam is unsolicited commercial e-mail advertising for products, services, and websites. Spam can also be used as a delivery mechanism for malicious software. Spam can appear in text messages as well as electronic mail. Besides the inconvenience of deleting spam, users may face charges for unwanted text messages. Spam can also be used for phishing attempts.
Spoofing	Attackers may create fraudulent websites to mimic or "spoof" legitimate sites and in some cases may use the fraudulent sites to distribute malware to mobile devices. E-mail spoofing occurs when the sender address and other parts of an e-mail header are altered to appear as though the e-mail originated from a different source. Spoofing hides the origin of an e-mail message. Spoofed e-mails may contain malware.
Theft/Loss	Because of their small size and use outside the office, mobile devices can be easier to misplace or steal than a laptop or notebook computer. If mobile devices are lost or stolen, it may be relatively easy to gain access to the information they store.
Zero-day exploit	A zero-day exploit takes advantage of a security vulnerability before an update for the vulnerability is available. By writing an exploit for an unknown vulnerability, the attacker creates a potential threat because mobile devices generally will not have software patches to prevent the exploit from succeeding.

APPENDIX C. DEFINITIONS OF KEY SECURITY CONTROLS

(From GAO, 2012)

Key Security Controls to Combat Common Mobile Threats and Vulnerabilities	
Security Control	**Description**
Enable user authentication	Devices can be configured to require passwords or PINs to gain access. In addition, the password field can be masked to prevent it from being observed, and the devices can activate idle-time screen locking to prevent unauthorized access.
Enable two-factor authentication for sensitive transactions	Two-factor authentication can be used when conducting sensitive transactions on mobile devices. Two-factor authentication provides a higher level of security than traditional passwords. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors"—something you know, something you have, or something you are—before being granted access. Mobile devices themselves can be used as a second factor in some two-factor authentication schemes used for remote access. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Two-factor authentication may be important when sensitive transactions occur, such as for mobile banking or conducting financial transactions.
Verify the authenticity of downloaded applications	Procedures can be implemented for assessing the digital signatures of downloaded applications to ensure that they have not been tampered with.
Install antimalware capability	Antimalware protection can be installed to protect against malicious applications, viruses, spyware, infected secure digital cards, and malware-based attacks. In addition, such capabilities can protect against unwanted (spam) voice messages, text messages, and e-mail attachments.
Install a firewall	A personal firewall can protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules.
Receive prompt security updates	Software updates can be automatically transferred from the manufacturer or carrier directly to a mobile device. Procedures can be implemented to ensure these updates are transmitted promptly.
Remotely disable lost or stolen devices	Remote disabling is a feature for lost or stolen devices that either locks the device or completely erases its contents remotely. Locked devices can be unlocked subsequently by the

	user if they are recovered.
Enable encryption for data stored on device or memory card	File encryption protects sensitive data stored on mobile devices and memory cards. Devices can have built-in encryption capabilities or use commercially available encryption tools.
Enable whitelisting	Whitelisting is a software control that permits only known safe applications to execute commands.

APPENDIX D. DEFINITIONS OF ADDITIONAL SECURITY CONTROLS

(From GAO, 2012)

Additional Security Controls to Combat Common Mobile Threats and Vulnerabilities	
Security Control	**Description**
Adopt centralized security management	Centralized security management can ensure an organization's mobile devices are compliant with its security policies. Centralized security management includes (1) configuration control, such as installing remote disabling on all devices; and (2) management practices, such as setting policy for individual users or a class of users on specific devices.
Use mobile device integrity validation software	Software tools can be used to scan devices for key compromising events (e.g., an unexpected change in the file structure) and then report the results of the scans, including a risk rating and recommended mitigation.
Implement a virtual private network (VPN)	A VPN can provide a secure communications channel for sensitive data transferred across multiple, public networks during remote access. VPNs are useful for wireless technologies because they provide a way to secure wireless local area networks, such as those at public Wi-Fi spots, in homes, or other locations.
Use public key infrastructure (PKI) support	PKI-issued digital certificates can be used to digitally sign and encrypt e-mails.
Require conformance to government specifications	Organizations can require that devices meet government specifications before they are deployed. For example, NIST recommends that mobile devices used in government enterprises adhere to a minimum set of security requirements for cryptographic modules that include both hardware and software components. The Defense Information Systems Agency has certified a secure Android-based mobile system for use by DoD agencies. The system allows DoD personnel to sign, encrypt and decrypt e-mail, and securely access data from a smartphone or tablet computer.
Install an enterprise firewall	An enterprise firewall can be configured to isolate all unapproved traffic to and from wireless devices.
Monitor incoming traffic	Enterprise information technology network operators can use intrusion prevention software to examine traffic entering the network from mobile devices.
Monitor and control	Devices can be monitored and controlled for messaging, data

devices	leakage, inappropriate use, and to prevent applications from being installed.
Enable, obtain, and analyze device log files for compliance	Log files can be reviewed to detect suspicious activity and ensure compliance.

APPENDIX E. DEFINITIONS OF KEY SECURITY PRACTICES

(From GAO, 2012)

Key Security Practices to Combat Common Mobile Threats and Vulnerabilities	
Security Practice	**Description**
Turn off or set Bluetooth connection capabilities to nondiscoverable	When in discoverable mode, Bluetooth-enabled devices are "visible" to other nearby devices, which may alert an attacker to target them. When Bluetooth is turned off or in nondiscoverable mode, the Bluetooth-enabled devices are invisible to other unauthenticated devices.
Limit use of public Wi-Fi networks when conducting sensitive transactions	Attackers may patrol public Wi-Fi networks for unsecured devices or even create malicious Wi-Fi spots designed to attack mobile phones. Public Wi-Fi spots represent an easy channel for hackers to exploit. Users can limit their use of public Wi-Fi networks by not conducting sensitive transactions when connected to them or if connecting to them, using secure, encrypted connections. This can help reduce the risk of attackers obtaining sensitive information such as passwords, bank account numbers, and credit card numbers.
Minimize installation of unnecessary applications	Once installed, applications may be able to access user content and device programming interfaces, and they may also contain vulnerabilities. Users can reduce risk by limiting unnecessary applications.
Configure web accounts to use secure connections	Accounts for many websites can be configured to use secure, encrypted connections. Enabling this feature limits eavesdropping on web sessions.
Do not follow links sent in suspicious e-mail or text messages	Users should not follow links in suspicious e-mail or text messages, because such links may lead to malicious websites.
Limit clicking on suspicious advertisements within an application	Suspicious advertisements may include links to malicious websites, prompting the users to download malware, or violate their privacy. Users can limit this risk by not clicking on suspicious advertisements within applications.
Limit exposure of mobile phone numbers	By not posting mobile phone numbers to public websites, users may be able to limit the extent to which attackers can obtain known mobile numbers to attack.
Limit storage of sensitive information on mobile devices	Users can limit storing of sensitive information on mobile devices.
Maintain physical control	Users can take steps to safeguard their mobile devices, such as by keeping their devices secured in a bag to reduce the risk that

	their mobile devices will be lost or stolen.
Delete all information stored in a device prior to discarding it	By using software tools that thoroughly delete (or "wipe") information stored in a device before discarding it, users can protect their information from unauthorized access.
Avoid modifying mobile devices	Modifying or "jailbreaking" mobile devices can expose them to security vulnerabilities or can prevent them from receiving security updates.

APPENDIX F. DEFINITIONS OF ADDITIONAL SECURITY PRACTICES

(From GAO, 2012)

Additional Security Practices to Combat Common Mobile Threats and Vulnerabilities	
Security Practice	**Description**
Establish a mobile device security policy	Security policies define the rules, principles, and practices that determine how an organization treats mobile devices, whether they are issued by the organization or owned by individuals. Policies should cover areas such as roles and responsibilities, infrastructure security, device security, and security assessments. By establishing policies that address these areas, agencies can create a framework for applying practices, tools, and training to help support the security of wireless networks.
Provide mobile device security training	Training employees in an organization's mobile security policies can help to ensure that mobile devices are configured, operated, and used in a secure and appropriate manner.
Establish a deployment plan	Following a well-designed deployment plan helps to ensure that security objectives are met.
Perform risk assessments	Risk analysis identifies vulnerabilities and threats, enumerates potential attacks, assesses their likelihood of success, and estimates the potential damage from successful attacks on mobile devices.
Perform configuration control and management	Configuration management ensures that mobile devices are protected against the introduction of improper modifications before, during, and after deployment.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX G. POSITION CATEGORY DESCRIPTIONS

(From DAU, 2013)

AT&L Workforce Position Category Description (PCD)

Career Field: Contracting (Including Construction)
Career Path: Not Uniquely Specified
Short Title CON
Category Code: C **Ref:** (a) DoDD 5000.52 dtd 12 Jan 2005
Date Approved: 9 Jun 2008 (b) DoDI 5000.66 dtd 21 Dec 2005
Last Reviewed: 9 April 2012 (c) DoD Desk Guide for AT&L Workforce Career Management dtd 10 Jan 2006

Notes:

1. This PCD is intended to assist in determining which AT&L career field/path to assign to an AT&L position per Title 10 sec. 1721. Civilian Series 1102 and their military counterparts as noted under Career Codes are always designated as acquisition and in the Contracting Career Field IAW reference (c)
2. All positions, regardless of location, function or series, requiring a warranted contracting officer above the (Simplified Acquisition Threshold) must be designated as an AT&L position in the contracting career field per 10 USC Chapter 87 sec 1724.
3. All acquisition positions require management attention with respect to certification requirements and individual development. See reference (c).
4. Critical Acquisition Positions (CAPs) are a subset of acquisition positions and Key Leadership Positions (KLPs), are a subset of CAPs. Both CAPs and KLPs represent positions with responsibility and authority that are critical to the success of a program or effort. These positions require management attention with respect to Acquisition Corps membership, tenure and other specific statutory requirements. See reference (c).

General Acquisition Related Duties: The conceptualization, initiation, design, development, test, contracting, production, deployment, logistical support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in, or in support of, military missions.

AT&L Career Field/Path Specific Duties:

- Develop alternatives to produce best value supplies and services, as well as manage all aspects of the life cycle of a contract or other vehicle (e.g., orders, basic ordering agreements etc.)
- Apply statutory and policy procurement-related requirements; support attainment of government socio-economic objectives; conduct market research; acquisition planning; cost and price analysis; solicitation and selection of sources; preparation, negotiation, and award of contracts through various methods to include negotiation; and perform all phases of contract administration, and terminate or close out of contracts.

Typical Line and Staff Position Titles: Administrative Contracting Officer, Contract Price and/or Cost Analyst, Contracting Officer, Contract Negotiator, Contract Specialist, Contract Manager, Contract Administrator, Contract Termination Specialist, Small Business Specialist, Procurement Analyst, Procuring Contracting Officer, and Termination Contracting Officer.

Typical Position Locations: Any DoD activity/organization performing contracting functions regardless of location.

Typical Career Codes:

Civilian Personnel	Uniformed Personnel			
OCC Series	Army AOC	Navy AQD	Air Force AFSC	Marine Corps MOS
1102	FA 51C MOS 51C	ACx	64PX 6C0X1	3006 8057 8060 3044 8058 8856

Recommended Changes/Updates: Forward to: Director, Learning Capabilities Integration Center (Attn: Dir, Academic Programs), Defense Acquisition University, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565 or call 703-805-4090

AT&L Workforce Position Category Description (PCD)

Career Field: Program Management
Career Path: Not Uniquely Specified
Short Title PM
Category Code: A
Date Approved: 12 Mar 2007
Last Reviewed: 1 Nov 2012

Ref: (a) DoDD 5000.52 dtd 12 Jan 2005
(b) DoDI 5000.66 dtd 21 Dec 2005
(c) DoD Desk Guide for AT&L Workforce Career Management dtd 10 Jan 2006

Notes:

1. This PCD is intended to assist in determining which AT&L career field/path to assign to an AT&L position per Title 10 sec. 1721. If 50% or more of the duties and responsibilities of the position match the "General Acquisition-Related Duties" described below AND the preponderance of those duties match the "AT&L Career Field/Path Specific Duties" described below, assign the position to this position category.
2. All acquisition positions require management attention with respect to certification requirements and individual development. See reference (c).
3. Critical Acquisition Positions (CAPs) are a subset of acquisition positions and Key Leadership Positions (KLPs), are a subset of CAPs. Both CAPs and KLPs represent positions with responsibility and authority that are critical to the success of a program or effort. These positions require management attention with respect to Acquisition Corps membership, tenure and other specific statutory requirements. See reference (c).

General Acquisition Related Duties: The conceptualization, initiation, design, development, test, contracting, production, deployment, logistical support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in, or in support of, military missions.

AT&L Career Field/Path Specific Duties:

- Manage a defense acquisition program. Responsibilities may be broad (e.g., PM, DPM, or PEO) or focused (e.g., Assistant PM for a particular function), and may be line or staff in nature.
- Execute duties guided by DoDD 5000.01, DoDI 5000.02, DoD Issuances governing acquisition programs in the DoD Components, and other program management policies addressed in DoD 5000 and 8000 series. Not covered in this category are basic research programs.

Typical Line and Staff Position Titles: CAE, PEO/Deputy, Program Director/Deputy, Program Manager/Deputy, Acquisition Manager, Project Officer, Materiel Wing/Group/Squadron Commander, Systems Sustainment Manager and Project Manager, Program Analyst, Program Integrator/Representative, IPT Lead.

Typical Position Locations: Acquisition organizations within the service components (i.e., Systems Commands, Materiel Commands, DRPMs. PEOs, as well as organizations/field activities directly supporting such organizations). Other DoD Components, Agencies and OSD/Service/HQ staff elements performing/supporting acquisition related functions, such as: DCMA; DLA.

Typical Career Codes:

Civilian Personnel	Uniformed Personnel			
OCC Series	**Army AOC**	**Navy AQD**	**Air Force AFSC**	**Marine Corps MOS**
0340 08xx 1515 0343 1101 06xx 13xx	51A 67	AAx	60CX 63AX	8057 8060 8058 8059

Recommended Changes/Updates: Forward to: Director, Leaning Capabilities Integration Center (Attn: Dir, Academic Programs), Defense Acquisition University, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565 or call 703-805-4090

Typical Career Codes:

Civilian Personnel	Uniformed Personnel			
OCC Series	**Army AOC**	**Navy AQD**	**Air Force AFSC**	**Marine Corps MOS**
0018 0660 13xx 0028 08xx 15xx 0301 1150 1910 0414 1152	51A 51C	AHx AGx	62 63	6002 8058 8869 75xx 8059 8057 8060

Recommended Changes/Updates: Forward to: Director, Learning Capabilities Integration Center (Attn: Dir, Academic Programs), Defense Acquisition University, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565 or call 703-805-4090

AT&L Workforce Position Category Description (PCD)

Career Field: Production, Quality & Manufacturing
Career Path: Not Specified
Short Title PQM
Category Code: H **Ref:** (a) DoDD 5000.52 dtd 12 Jan 2005
Date Approved: 20 Jul 2009 (b) DoDI 5000.66 dtd 21 Dec 2005
Last Reviewed: 12 Apr 2010 (c) DoD Desk Guide for AT&L Workforce Career Management dtd 10 Jan 2006

Notes:

1. This PCD is intended to assist in determining which AT&L career field/path to assign to an AT&L position per Title 10 sec. 1721. If 50% or more of the duties and responsibilities of the position match the "General Acquisition-Related Duties" described below AND the preponderance of those duties match the "AT&L Career Field/Path Specific Duties" described below, assign the position to this position category.
2. All acquisition positions require management attention with respect to certification requirements and individual development. See reference (c).
3. Critical Acquisition Positions (CAPs) are a subset of acquisition positions and Key Leadership Positions (KLPs), are a subset of CAPs. Both CAPs and KLPs represent positions with responsibility and authority that are critical to the success of a program or effort. These positions require management attention with respect to Acquisition Corps membership, tenure and other specific statutory requirements. See reference (c).

General Acquisition Related Duties: The conceptualization, initiation, design, development, test, contracting, production, deployment, logistical support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in, or in support of, military missions.

AT&L Career Field/Path Specific Duties: The specific duties fall into one or both of the following categories within this career field:

Production & Manufacturing:

Monitors and manages the manufacturing and production efforts at industry or Government facilities throughout the system acquisition process.
Assesses and reports on the availability of resources for production and realistic industry approaches to manufacturing and supply chain management.
Conducts feasibility assessments of risk during transition period and throughout the acquisition process.
Provides advice, assistance and recommendations to support "make" or "buy" decisions and alternative production processes.

Quality Assurance:

Manages Quality Assurance (QA) processes to establish essential quality standards and controls.
Develops, executes and evaluates policies, procedures, plans and test provisions for QA requirements throughout the various phrases of the systems acquisition cycle.
Ensures QA plans are integrated into the systems engineering process.
Performs process and product-oriented reviews and audits to ensure compliance with QA requirements
Provides expert support and guidance on QA-related matters to other program office and in-plant functional acquisition personnel.
Accepts and fields Materiel for U.S. and foreign customers.

Typical Line and Staff Position Titles:

Production & Manufacturing: Supervisory, Production, Manufacturing, Industrial Engineer; Production Management, Industrial Specialist; Production Officer; General, Aerospace, Mechanical Engineer.

Quality Assurance: QA Supervisor, Representative, or Staff Specialist; Mathematical Statistician, QA Engineer, Supervisory and/or Quality Engineer, Supervisory and/or General Engineer, Pharmacist, Physical Scientist, Chemist, Electronic Technician, Product Line Specialist (PLS), QA Director/ Chief (Division, Branch or Section); QA Surveillance Representative/Specialist, Engineer Technician, Entomologist, Computer Specialist, Product Auditor; Aircraft, Aerospace, Ammunition, Automotive, Chemicals, Clothing, Electronics, Materiel, Mechanical, Medical, Nuclear, Processes, Shipbuilding, Computer Software, or Subsistence.

Typical Position Locations: Acquisition organizations within the service components (i.e., Systems Commands, Materiel Commands, DRPMs. PEOs, as well as organizations/field activities directly supporting such organizations). Other DoD Components, Agencies and OSD/Service/HQ staff elements performing/supporting acquisition related functions such as DCMA, DLA and plant offices and component program offices.

Typical Career Codes:

Civilian Personnel	Uniformed Personnel			
OCC Series	Army AOC	Navy AQD	Air Force AFSC	Marine Corps MOS
0018 0660 13xx 0028 08xx 15xx 0301 1150 1910 0414 1152	51A 51C	AHx AGx	62 63	6002 8058 8869 75xx 8059 8057 8060

Recommended Changes/Updates: Forward to: Director, Learning Capabilities Integration Center (Attn: Dir, Academic Programs), Defense Acquisition University, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565 or call 703-805-4090

AT&L Workforce Position Category Description (PCD)

Career Field: Science & Technology Manager
Career Path:
Short Title S&TM
Category Code: I **Ref:** (a) DoDD 5000.52 dtd 12 Jan 2005
Date Approved: 2 Jan 2013 (b) DoDI 5000.66 dtd 21 Dec 2005
Last Reviewed: 2 Jan 2013 (c) DoD Desk Guide for AT&L Workforce Career Management dtd 10 Jan 2006

Notes:
1. This PCD is intended to assist in determining which AT&L career field/path to assign to an AT&L position per Title 10 sec. 1721. If 50% or more of the duties and responsibilities of the position match the "General Acquisition-Related Duties" described below AND the preponderance of those duties match the "AT&L Career Field/Path Specific Duties" described below, assign the position to this position category.
2. All acquisition positions require management attention with respect to certification requirements and individual development. See reference (c).
3. Critical Acquisition Position (CAPs) are a subset of acquisition positions and Key Leadership Position (KLPs), are a subset of CAPs. Both CAPs and KLPs represent positions with responsibility and authority that are critical to the success of a program or effort. These positions require management attention with respect to Acquisition Corps membership, tenure and other specific statutory requirements. See reference (c).

General Acquisition Related Duties: The conceptualization, initiation, design, development, test, contracting, production, deployment, logistical support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in, or in support of, military missions.

AT&L Career Field/Path Specific Duties:
- Develop overall program goals using S&T funds.
- Acquire the services of scientists, engineers and technical support personnel, experts in their fields, to perform science and technology research for DoD.
- Provide funds and oversee S&T performers including universities, industry, and Federal Government organizations.
- Interface with the technology customer(s) to expedite the transition of technology to the user.

Typical Line and Staff Position Titles: Technical Director, Scientist, Engineer, Project Engineer, Software Engineer

Typical Position Locations: Service component organizations such as: ARI, ARL, ARO and Research Development and Engineering Centers for the Army; ONR, NRL, and Warfare Centers for the Navy; AFOSR, AFRL for the Air Force and Fourth Estate organizations such as DTRA and NGA.

Typical Career Codes:

Civilian Personnel	Uniformed Personnel			
OCC Series	Army AOC	Navy AQD	Air Force AFSC	Marine Corps MOS
0180 08xx 15xx 04xx 13xx	51S 51T	Alx	61SX 62EX	8006 8058

Recommended Changes/Updates: Forward to: Director, Learning Capabilities Integration Center (Attn: Dir, Academic Programs), Defense Acquisition University, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565 or call 703-805-4090

AT&L Workforce Position Category Description (PCD)

Career Field: Systems Planning, Research, Development & Engineering
Career Path: Program Systems Engineer
Short Title SPRDE – PSE
Category Code: W **Ref:** (a) DoDD 5000.52 dtd 12 Jan 2005
Date Approved: 28 Sep 2010 (b) DoDI 5000.66 dtd 21 Dec 2005
Last Reviewed: 30 Aug 2012 (c) DoD Desk Guide for AT&L Workforce Career Management dtd 10 Jan 2006

Notes:
1. This PCD is intended to assist in determining which AT&L career field/path to assign to an AT&L position per Title 10 sec. 1721. If 50% or more of the duties and responsibilities of the position match the "General Acquisition-Related Duties" described below AND the preponderance of those duties match the "AT&L Career Field/Path Specific Duties" described below, assign the position to this position category.
2. All acquisition positions require management attention with respect to certification requirements and individual development. See reference (c).
3. Critical Acquisition Position (CAPs) are a subset of acquisition positions and Key Leadership Position (KLPs), are a subset of CAPs. Both CAPs and KLPs represent positions with responsibility and authority that are critical to the success of a program or effort. These positions require management attention with respect to Acquisition Corps membership, tenure and other specific statutory requirements. See reference (c).

General Acquisition Related Duties: The conceptualization, initiation, design, development, test, contracting, production, deployment, logistical support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in, or in support of, military missions.

AT&L Career Field/Path Specific Duties: Plan, manage, or perform analysis, research, design, development, fabrication, installation, modification, or sustainment of systems or systems components across the entire life cycle;

Apply most or all of the DoD Systems Engineering Technical Processes or Technical Management Processes (See Defense Acquisition Guide, Chapter 4, Section. 4.2) integrating multiple domains (analytic or engineering specialties) at a system or systems-of-systems level.

Technical Processes:
- stakeholders requirements definition
- requirements analysis
- architectural design
- implementation
- integration
- verification
- validation
- transition

Technical Management Processes:
- decision analysis
- technical planning
- technical assessment
- requirements management
- risk management
- configuration mgt
- technical data mgt
- interface management

Typical Line and Staff Position Titles: Systems Engineer, Lead/Chief Systems Engineering, System Engineer IPT Lead, Technical Director, Asst PEO/PM for SE.

Typical Position Locations: Acquisition organizations within the service components (i.e., Systems Commands, Material Commands, DRPMs, PEOs, as well as organizations/field activities directly supporting such organizations). Other DoD Components, Agencies and OSD/Service/HQ staff elements performing/supporting acquisition related functions, such as: DCMA; research, development, and engineering centers and laboratories; and manufacturing and maintenance centers and facilities.

Typical Career Codes:

Civilian Personnel	Uniformed Personnel			
OCC Series	**Army AOC**	**Navy AQD**	**Air Force AFSC**	**Marine Corps MOS**
0180 08xx 15xx 04xx 13xx	51S	AWx	61SX 62EX	72xx 8059 8832 75xx 8820 8836 8057 8824 8058 8826

Recommended Changes/Updates: Forward to: Director, Learning Capabilities Integration Center (Attn: Dir, Academic Programs), Defense Acquisition University, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565 or call 703-805-4090

AT&L Workforce Position Category Description (PCD)

Career Field: Systems Planning, Research, Development & Engineering
Career Path: Systems Engineering
Short Title SPRDE – SE
Category Code: S **Ref:** (a) DoDD 5000.52 dtd 12 Jan 2005
Date Approved: 28 Sep 2010 (b) DoDI 5000.66 dtd 21 Dec 2005
Last Reviewed: 30 Aug 2012 (c) DoD Desk Guide for AT&L Workforce Career Management dtd 10 Jan 2006

Notes:
1. This PCD is intended to assist in determining which AT&L career field/path to assign to an AT&L position per Title 10 sec. 1721. If 50% or more of the duties and responsibilities of the position match the "General Acquisition-Related Duties" described below AND the preponderance of those duties match the "AT&L Career Field/Path Specific Duties" described below, assign the position to this position category.
2. All acquisition positions require management attention with respect to certification requirements and individual development. See reference (c).
3. Critical Acquisition Position (CAPs) are a subset of acquisition positions and Key Leadership Position (KLPs), are a subset of CAPs. Both CAPs and KLPs represent positions with responsibility and authority that are critical to the success of a program or effort. These positions require management attention with respect to Acquisition Corps membership, tenure and other specific statutory requirements. See reference (c).

General Acquisition Related Duties: The conceptualization, initiation, design, development, test, contracting, production, deployment, logistical support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in, or in support of, military missions.

AT&L Career Field/Path Specific Duties: Plan, manage, or perform analysis, research, design, development, fabrication, installation, modification, or sustainment of systems or systems components across the entire life cycle;

Apply one or more of the DoD Systems Engineering Technical Processes or Technical Management Processes (See Defense Acquisition Guide, Chapter 4, Section. 4.2) for a specific domain (analytic or engineering specialty) at a subsystem or component level

Technical Processes:
- stakeholders requirements definition
- requirements analysis
- architectural design
- implementation
- integration
- verification
- validation
- transition

Technical Management Processes:
- decision analysis
- technical planning
- technical assessment
- requirements management
- risk management
- configuration management
- technical data management
- interface management.

Typical Line and Staff Position Titles: Project officer, project engineer, scientist, supervising project engineer, computer engineer/scientist, operations research analyst, software engineer, naval architect, specialty engineers such as materials or structures engineer, reliability engineer, designing engineer, cost engineer.

Typical Position Locations: Acquisition organizations within the service components (i.e., Systems Commands, Materiel Commands, DRPMs. PEOs, as well as organizations/field activities directly supporting such organizations). Other DoD Components, Agencies and OSD/Service/HQ staff elements performing/supporting acquisition related functions such as: DCMA; research, development, and engineering centers and laboratories; manufacturing and maintenance centers and facilities.

Typical Career Codes:

Civilian Personnel	Uniformed Personnel			
OCC Series	**Army AOC**	**Navy AQD**	**Air Force AFSC**	**Marine Corps MOS**
0180 15xx 04xx 08xx 13xx	51S	ASx	61SX 62EX	72xx 8059 8832 75xx 8820 8836 8057 8824 8058 8826

Recommended Changes/Updates: Forward to: Director, Learning Capabilities Integration Center (Attn: Dir, Academic Programs), Defense Acquisition University, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565 or call 703-805-4090

AT&L Workforce Position Category Description (PCD)

Career Field: Test and Evaluation
Career Path: Not Uniquely Specified
Short Title T&E
Category Code: T **Ref:** (a) DoDD 5000.52 dtd 12 Jan 2005
Date Approved: 1 Jun 2012 (b) DoDI 5000.66 dtd 21 Dec 2005
Last Reviewed: 1 Jun 2012 (c) DoD Desk Guide for AT&L Workforce Career Management dtd 10 Jan 2006

Notes:
1. This PCD is intended to assist in determining which AT&L career field/path to assign to an AT&L position per Title 10 sec. 1721. If 50% or more of the duties and responsibilities of the position match the "General Acquisition-Related Duties" described below **AND** the preponderance of those duties match the "AT&L Career Field/Path Specific Duties" described below, assign the position to this position category.
2. All acquisition positions require management attention with respect to certification requirements and individual development. See reference (c).
3. Critical Acquisition Positions (CAPs) are a subset of acquisition positions and Key Leadership Positions (KLPs), are a subset of CAPs. Both CAPs and KLPs represent positions with responsibility and authority that are critical to the success of a program or effort. These positions require management attention with respect to Acquisition Corps membership, tenure and other specific statutory requirements. See reference (c).

General Acquisition Related Duties: The conceptualization, initiation, design, development, test, contracting, production, deployment, logistical support, modification, and disposal of weapons and other systems, supplies, or services (including construction) to satisfy DoD needs, intended for use in, or in support of, military missions.

AT&L Career Field/Path Specific Duties:
- Serves as Chief Developmental Tester for MDAP or MAIS.
- Serves as the Chair, T&E Working-Level Integrated Product Team (T&E WIPT), or member representing the materiel developer, tester, and / or system evaluator.
- Analyzes requirements/capabilities documents to determine testability and measurability.
- Plan, organize, manage, or conduct test and/or evaluation associated with concepts, emerging technologies, and experiments as well as prototypes, new, fielded, or modified C4ISR systems (including IT systems participating in system of systems (SoS), family of systems (FoS), and net-centric services), weapon or automated information systems, equipment or materiel throughout all acquisition phases to include developmental tests, and support to in-service tests and operational tests.
- Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated; analyze, assess, and evaluate test data/results; prepare reports of system performance and T&E findings.
- Develop T&E processes, modify, adapt, tailor, or extend standard T&E guides, precedents, criteria, methods, and techniques, to include Design of Experiments, M&S and Information Assurance T&E and certification.
- Design and use existing or new test equipment, procedures, and approaches.
- Write, edit, and staff a T&E Strategy (TES) or T&E Master Plan (TEMP), as well as system-level and / or individual element test plans.
- Conduct development T&E, and support operational tests, and evaluate and / or analyze test results and /or test data; and prepare and present evaluation/assessment results.
- Categorize test data, equipment, materiel, or system deficiencies and certify readiness for OT&E.

Typical Line and Staff Position Titles: Chief Developmental Tester; Chair, T&E Working-level IPT; Assistant PEO for T&E; Assistant PM for T&E; Lead Test Engineer; Lead Experimentation Engineer; Chief Test Engineer; Chief Test Pilot; Test Director/Manager; Test Engineer; Acquisition T&E Department Head; Director, Flight Test Engineering; Test and Experimentation Design Branch Head; T&E Department Head, Capability Test Team Chair; Portfolio Manager; Chief Test Officer; Test Officer; T&E Analyst; Lead Simulator Engineer.

Typical Position Locations: Lead Developmental Test and Evaluation Organization; Service and Defense Agency test centers, major range and test facility base (MRTFB) test facilities, warfare centers, laboratories as well as OSD/Service/HQ staff elements, field activities, and acquisition organizations within the Service components (e.g., Systems Commands, Materiel Commands, DRPMs, PEOs, and PM Offices).

Typical Career Codes:

Civilian Personnel	Uniformed Personnel							
OCC Series	Army AOC	Navy AQD	Air Force AFSC		Marine Corps MOS		
08xx	51A	ATx	11XX	61XX	1302	8057	8824
13xx	51T		12XX	62EX	1802	8058	8826
15xx			13XX	63AX	72xx	8059	8832
			17DX		75xx	8820	8836

Recommended Changes/Updates: Forward to: Director, Learning Capabilities Integration Center (Attn: Dir, Academic Programs), Defense Acquisition University, 9820 Belvoir Road, Suite 3, Fort Belvoir, VA 22060-5565 or call 703-805-4090

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX H. TECHNOLOGY READINESS LEVELS

(From DRD DDR&E , 2009)

The following matrix lists the various technology readiness levels and descriptions from a systems approach for both hardware and software. DoD Components may provide additional clarifications for software. Supplemental definitions follow the table.

Technology Readiness Level	**Description**
1. Basic principles observed and reported	Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.
2. Technology concept and/or application formulated	Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.
3. Analytical and experimental critical function and/or characteristic proof of concept	Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.
4. Component and/or breadboard validation in laboratory environment	Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of ad hoc hardware in the laboratory.
5. Component and/or breadboard validation in relevant environment	Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of

	components.
6. System/subsystem model or prototype demonstration in a relevant environment	Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in a simulated operational environment.
7. System prototype demonstration in an operational environment	Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.
8. Actual system completed and qualified through test and demonstration	Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.
9. Actual system proven through successful mission operations	Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

DEFINITIONS

BREADBOARD: Integrated components that provide a representation of a system/subsystem and which can be used to determine concept feasibility and to develop technical data. Typically configured for laboratory use to demonstrate the technical principles of immediate interest. May resemble final system/subsystem in function only.

"HIGH FIDELITY": Addresses form, fit and function. High-fidelity laboratory environment would involve testing with equipment that can simulate and validate all system specifications within a laboratory setting.

“LOW FIDELITY”: A representative of the component or system that has limited ability to provide anything but first order information about the end product. Low-fidelity assessments are used to provide trend analysis.

MODEL: A functional form of a system, generally reduced in scale, near or at operational specification. Models will be sufficiently hardened to allow demonstration of the technical and operational capabilities required of the final system.

OPERATIONAL ENVIRONMENT: Environment that addresses all of the operational requirements and specifications required of the final system to include platform/packaging.

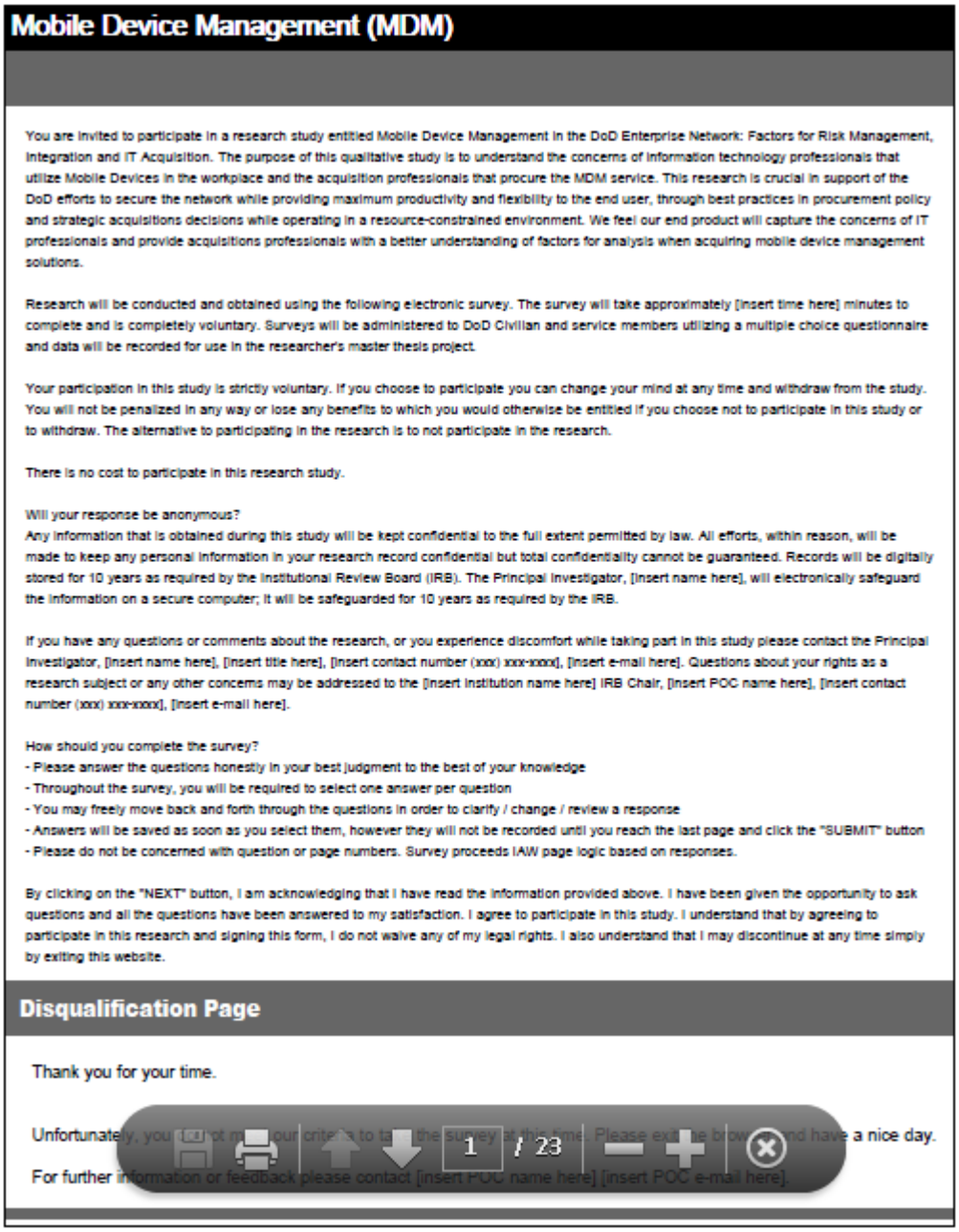
PROTOTYPE: A physical or virtual model used to evaluate the technical or manufacturing feasibility or military utility of a particular technology or process, concept, end item or system.

RELEVANT ENVIRONMENT: Testing environment that simulates the key aspects of the operational environment.

SIMULATED OPERATIONAL ENVIRONMENTAL: Either 1) a real environment that can simulate all of the operational requirements and specifications required of the final system, or 2) a simulated environment that allows for testing of a virtual prototype; used in either case to determine whether a developmental system meets the operational requirements and specifications of the final system.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I. USER SURVEY



Mobile Device Management (MDM)

You are invited to participate in a research study entitled Mobile Device Management in the DoD Enterprise Network: Factors for Risk Management, Integration and IT Acquisition. The purpose of this qualitative study is to understand the concerns of information technology professionals that utilize Mobile Devices in the workplace and the acquisition professionals that procure the MDM service. This research is crucial in support of the DoD efforts to secure the network while providing maximum productivity and flexibility to the end user, through best practices in procurement policy and strategic acquisitions decisions while operating in a resource-constrained environment. We feel our end product will capture the concerns of IT professionals and provide acquisitions professionals with a better understanding of factors for analysis when acquiring mobile device management solutions.

Research will be conducted and obtained using the following electronic survey. The survey will take approximately [insert time here] minutes to complete and is completely voluntary. Surveys will be administered to DoD Civilian and service members utilizing a multiple choice questionnaire and data will be recorded for use in the researcher's master thesis project.

Your participation in this study is strictly voluntary. If you choose to participate you can change your mind at any time and withdraw from the study. You will not be penalized in any way or lose any benefits to which you would otherwise be entitled if you choose not to participate in this study or to withdraw. The alternative to participating in the research is to not participate in the research.

There is no cost to participate in this research study.

Will your response be anonymous?
Any information that is obtained during this study will be kept confidential to the full extent permitted by law. All efforts, within reason, will be made to keep any personal information in your research record confidential but total confidentiality cannot be guaranteed. Records will be digitally stored for 10 years as required by the Institutional Review Board (IRB). The Principal Investigator, [insert name here], will electronically safeguard the information on a secure computer; it will be safeguarded for 10 years as required by the IRB.

If you have any questions or comments about the research, or you experience discomfort while taking part in this study please contact the Principal Investigator, [insert name here], [insert title here], [insert contact number (xxx) xxx-xxxx], [insert e-mail here]. Questions about your rights as a research subject or any other concerns may be addressed to the [insert institution name here] IRB Chair, [insert POC name here], [insert contact number (xxx) xxx-xxxx], [insert e-mail here].

How should you complete the survey?
- Please answer the questions honestly in your best judgment to the best of your knowledge
- Throughout the survey, you will be required to select one answer per question
- You may freely move back and forth through the questions in order to clarify / change / review a response
- Answers will be saved as soon as you select them, however they will not be recorded until you reach the last page and click the "SUBMIT" button
- Please do not be concerned with question or page numbers. Survey proceeds IAW page logic based on responses.

By clicking on the "NEXT" button, I am acknowledging that I have read the information provided above. I have been given the opportunity to ask questions and all the questions have been answered to my satisfaction. I agree to participate in this study. I understand that by agreeing to participate in this research and signing this form, I do not waive any of my legal rights. I also understand that I may discontinue at any time simply by exiting this website.

Disqualification Page

Thank you for your time.

Unfortunately, you do not meet our criteria to take the survey at this time. Please exit the browser and have a nice day.

For further information or feedback please contact [insert POC name here] [insert POC e-mail here].

1 / 23

Mobile Device Management (MDM)

MDM - Part 1 Demographics

This is a great opportunity to express your opinion and provide suggestions. Your answers will be critical in developing future strategies. We encourage you to answer each question to the best of your ability.

The survey contains 2 parts. Part 1 is General Demographics. Part 2 is comprised of questions specifically on MDM.

1. Please pick the best option that describes you.

- Uniformed Service
- Federal Civilian
- DoD Contractor

Service

2. Please select your Service

- Army
- Air Force
- Navy
- Marines
- Coast Guard

Other (please specify)

Military Pay Grade

3. Please specify your pay grade.

- O1
- O2
- O3
- O4
- O5
- O6
- O7
- O8
- O9
- O10
- WO1
- WO2
- WO3
- WO4
- WO5
- E1
- E2
- E3
- E4
- E5
- E6
- E7
- E8
- E9

Other (please specify)

Civilian Pay Grade

Mobile Device Management (MDM)

4. Please specify your pay grade.

- GS1
- GS2
- GS3
- GS4
- GS5
- GS6
- GS7
- GS8
- GS9
- GS10
- GS11
- GS12
- GS13
- GS14
- GS15
- SESI
- SESII
- SESIII
- SESIV
- SESV

Other (please specify)

Agency / Organization / Unit

5. Please select your Agency / Organization / Unit.

- DISA
- CERDEC
- NSA
- DHS
- MITRE
- NIST
- RDECOM

Other (please specify)

6. Please pick the best option that describes you.

- Information Technology Professional (Ie SA, NA, SME)
- Acquisition Professional (Ie KO, PM, 2210)
- Information Assurance (Ie IASM, IASO, Crypto)
- Information Technology Manager (Ie CIO, CTO, DAA)

Other or Comment (please specify)

DAWIA Certification

Mobile Device Management (MDM)

7. What is your primary DAWIA certification?

- Contracting
- PQM
- SPRDE-S&TM
- Information Technology
- Program Management
- SPRDE-SE
- Life Cycle Logistics
- SPRDE-PSE
- Test and Evaluation

Other (please specify)

MDM - Target Knowledge

8. Do you believe that you have sufficient product experience / knowledge in order to contribute to the expansion of DoD's knowledge in regards to Mobile Device Management?

- Yes
- No

MDM - Qualification Page

You meet our survey respondent criteria and may fill out the response to the following questions.

Thank you for your help, support, and service.

MDM - Target Knowledge

9. To what extent does your unit / agency / organization provide training to IT / AC / IS professionals on MDM?

- To a large extent
- To a moderate extent
- To some extent
- To little extent
- Not at all

Comment / Remarks

Mobile Device Management (MDM)

10. What type of training do you require to become proficient in MDM? (check all that apply)

- ☐ IOS and Android operations systems
- ☐ Information Security
- ☐ Types of Material Solutions
- ☐ Bring Your Own Device (BYOD)
- ☐ Cost Benefit Analysis

Other (please specify)

MDM - Part 2 Functional Requirements

In the following series of questions we will attempt to gather input on four functional requirements of MDM systems.

Software Distribution is defined as:
the ability to manage and support mobile application use including deploy, install, update, delete or block.

Policy Management is defined as:
the development, control and operations of DoD enterprise mobile access, connectivity, and security policy.

Inventory Management is defined as:
the software, firmware, hardware, and peripheral device inventory management, this includes provisioning and support.

Security Management is defined as:
the implementation and enforcement of DoD-level device security, authentication, validation and encryption functionality.

MDM Attribute - Policy Management

In the following questions we will attempt to gather the importance of the possible attributes of a MDM system.

Policy Management is defined as:
the development, control and operations of DoD enterprise mobile access, connectivity, and security policy.

Mobile Device Management (MDM)

11. How important are the following attributes for Policy Management to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
Administer policies as groups	☐	☐	☐	☐	☐
Administer policies as individuals	☐	☐	☐	☐	☐
Complex password enforcement (strong alphanumeric password)	☐	☐	☐	☐	☐
Enable browser enforcement through DoD proxy	☐	☐	☐	☐	☐
Enforce URL and web content filtering	☐	☐	☐	☐	☐
Support complex group policies (multi-layered, hierarchical, etc.) and/or individual policies	☐	☐	☐	☐	☐
Support granular restrictive access to specific public app repositories and/or specific applications on specific public app repositories	☐	☐	☐	☐	☐

Comment / Remarks

MDM - Policy Management

Policy Management is defined as:
the development, control and operations of DoD enterprise mobile access, connectivity, and security policy.

Mobile Device Management (MDM)

12. How important are the following attributes for Policy Management to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
Alert system for users and IT administrators when device policies are violated, which includes the ability to "kill" devices when they become non-compliant	☐	☐	☐	☐	☐
Enforce DoD Logon Banner or custom text to device lock	☐	☐	☐	☐	☐
Force exclusive use of VPN for all IP traffic	☐	☐	☐	☐	☐
Policy compliance reporting	☐	☐	☐	☐	☐
Query for compliance and security information	☐	☐	☐	☐	☐
Restrict access to enterprise servers	☐	☐	☐	☐	☐

Comment / Remarks

MDM Attributes - Security Management

Security Management is defined as:
the implementation and enforcement of DoD-level device security, authentication, validation and encryption functionality.

Mobile Device Management (MDM)

13. How important are following attributes for Security Management to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
Administrator / remote reset of device password	☐	☐	☐	☐	☐
CAC/PIV device authentication	☐	☐	☐	☐	☐
Device lock (after a given period of inactivity)	☐	☐	☐	☐	☐
Disable automatic connection to WI-FI networks	☐	☐	☐	☐	☐
Disable infrared (IR) port	☐	☐	☐	☐	☐
Disable WI-FI radio	☐	☐	☐	☐	☐
Remote device lock	☐	☐	☐	☐	☐
Remote device wipe (both selective and total)	☐	☐	☐	☐	☐

Comment / Remarks

MDM Attributes - Security Management

Mobile Device Management (MDM)

14. How important are following attributes for Security Management to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
Bluetooth profile whitelist/blacklist by peripheral type	☐	☐	☐	☐	☐
Bluetooth profile whitelist/blacklist by vendor	☐	☐	☐	☐	☐
Disable Bluetooth radio	☐	☐	☐	☐	☐
Disable camera(s)	☐	☐	☐	☐	☐
Disable cellular radio	☐	☐	☐	☐	☐
Disable microphone(s)	☐	☐	☐	☐	☐
Disable removable media port	☐	☐	☐	☐	☐

Comment / Remarks

MDM Attributes - Security Management

Mobile Device Management (MDM)

15. How important are following attributes for Security Management to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
Disable access to public app repositories (i.e. App Store, Android Market, etc.)	☐	☐	☐	☐	☐
Disable Location-based services (GPS)	☐	☐	☐	☐	☐
Disable screen capture	☐	☐	☐	☐	☐
Disable USB/serial port (i.e. 30-pin dock connector, MicroUSB, MiniUSB, etc.)	☐	☐	☐	☐	☐
Disable use of preinstalled browser	☐	☐	☐	☐	☐
Disable voice dialing	☐	☐	☐	☐	☐
Support restrictive management of USB/serial access by vendor and/or peripheral type	☐	☐	☐	☐	☐

Comment / Remarks

MDM Attributes - Inventory Management

In the following questions we will attempt to gather the importance of the following possible attributes of a MDM system.

Inventory Management is defined as:
the software, firmware, hardware, and peripheral device inventory management, this includes provisioning and support.

Mobile Device Management (MDM)

16. How important are the following attributes of Inventory Management to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
Device activation and deactivation	☐	☐	☐	☐	☐
Device configuration and imaging	☐	☐	☐	☐	☐
Enforce mobile communication expense policies, such as disabling cellular data or access to servers when roaming internationally	☐	☐	☐	☐	☐
Query support for device and network information	☐	☐	☐	☐	☐
Trouble ticket and tracking management	☐	☐	☐	☐	☐

Comment / Remarks

MDM Attributes - Software Distribution

In the following questions we will attempt to gather the importance of the following possible attributes of a MDM system.

Software Distribution is defined as:
the ability to manage and support mobile application use including deploy, install, update, delete or block.

Mobile Device Management (MDM)

17. How important are the following attributes of Software Distribution to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
Access to private application repository	☐	☐	☐	☐	☐
Backup/restore of configuration data	☐	☐	☐	☐	☐
Backup/restore of software	☐	☐	☐	☐	☐
Push and/or pull over-the-air (OTA) software updates for applications and Operating Systems (OSes)	☐	☐	☐	☐	☐
Trusted controls for over-the-air (OTA) or tethered provisioning and updating process	☐	☐	☐	☐	☐

Comment / Remarks

MDM Additional Function - Malware Control Management

In the following questions we will attempt to gather the importance of the following possible attributes of a MDM system.

18. How important are the following attributes of Malware Control Mangement to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
Antivirus and malware detection	☐	☐	☐	☐	☐
Phishing protection	☐	☐	☐	☐	☐
Spam protection	☐	☐	☐	☐	☐

Comment / Remarks

MDM Additional Function - Email

In the following questions we will attempt to gather the importance of the following possible attributes of a MDM system.

Mobile Device Management (MDM)

19. How important are the following attributes of E-mail to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
CAC/PIV encryption and signing integration	☐	☐	☐	☐	☐
DoD Global Address List (GAL) integration	☐	☐	☐	☐	☐
Integrated calendaring	☐	☐	☐	☐	☐
Plain text only native email enforcement	☐	☐	☐	☐	☐
S/MIME capability	☐	☐	☐	☐	☐

Comment / Remarks

MDM Additional Function - VPN Management

In the following questions we will attempt to gather the importance of the following possible attributes of a MDM system.

20. How important are the following attributes of VPN Management to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
Disable Split Tunneling	☐	☐	☐	☐	☐
FIPS 140-2 data-in-transit encryption	☐	☐	☐	☐	☐
IPSec/SSL end-to-end encryption	☐	☐	☐	☐	☐
PKI-based authentication	☐	☐	☐	☐	☐

Comment / Remarks

MDM Additional Function - Administration and Reporting

In the following questions we will attempt to gather the importance of the following possible attributes of a MDM system.

Mobile Device Management (MDM)

21. How important are the following attributes of Administration and Reporting to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
A Certificate of Networthiness (CoN)	☐	☐	☐	☐	☐
Access to management server via single or web-based console Role-based access	☐	☐	☐	☐	☐
Business intelligence, analytics, and reporting tools	☐	☐	☐	☐	☐
Enterprise platform integration (i.e. LDAP, Blackberry Enterprise Server, Good Mobile Messaging, certificate authority, trouble ticketing and help desk, such as Remedy)	☐	☐	☐	☐	☐
FIPS 140-2 level 1 encryption of administrative (MDM) communications	☐	☐	☐	☐	☐
Group-based action management	☐	☐	☐	☐	☐
Integration of hard and/or soft token user authentication, i.e. Common Access Card (CAC), microSD, near-field communication (NFC), etc.	☐	☐	☐	☐	☐

Comment / Remarks

MDM - Functional Ranking

Mobile Device Management (MDM)

22. How important to you are the following functions to MDM:

	Very Important	Somewhat Important	Neither Important nor Unimportant	Somewhat Unimportant	Very Unimportant
Administration and Reporting	☐	☐	☐	☐	☐
Email	☐	☐	☐	☐	☐
Inventory Management	☐	☐	☐	☐	☐
Malware Control Management	☐	☐	☐	☐	☐
Policy Management	☐	☐	☐	☐	☐
Security Management	☐	☐	☐	☐	☐
Software Distribution	☐	☐	☐	☐	☐
VPN Management	☐	☐	☐	☐	☐

Comment / Remarks

MDM - Operating Model

In the following questions, we are attempting to gather your opinion on the Operating Model associated with MDM systems.

The definition of a operating model is as follows:
the necessary level of business process integration and standardization for delivering goods and services to customers.

In the case of MDM:
- goods and services is generalized as telecom and data applications
- Customer are the users IE Soldiers and or Federal Civilians

Mobile Device Management (MDM)

23. What best describes your organizations operating model:

REPLICATION: - Few, if any, shared customers - Independent transactions aggregated at a high level - Operationally similar business units - Autonomous similar business unit leaders with limited discretion over processes - Centralized control over business process design - Standardized data definitions but data locally owned with some aggregation at corporate - Centrally mandated IT services

UNIFICATION: - Customers and suppliers may be local or global - Globally integrated business processes often with support of enterprise systems - Business units with similar or overlapping operations - Centralized management often applying functional / process / business unit matrices - High level process owners design standardized processes - Centrally mandated databases - IT decisions made centrally

DIVERSIFICATION: - Few, in any shared customers or suppliers - Independent transactions - Operationally unique business units - Autonomous business management - Business unit control over business process design - Few data standards across business units - Most IT decisions made within business units

COORDINATION: - Shared customers, products, or services - Impact on other business unit transaction - Operationally unique business units or functions - Autonomous business management - Shared customer / supplier / product data - Consensus processes for designing IT infrastructure services; IT applications decisions made in business units

Other (please specify)

MDM- Operating Model

24. How dependent is your unit / agency / organization transactions dependent on the availability, accuracy, and timeliness of other units / agencies / organizations data?

Not Very Dependent | Somewhat Dependent | Dependent | Very Dependent | Extremely Dependent

Other (please specify)

25. How beneficial to your unit / agency / organization is it for your individual units / agencies / organizations to run their operations in the same way?

Not Very Beneficial | Somewhat Beneficial | Beneficial | Very Beneficial | Extremely Beneficial

Other (please specify)

MDM - Technology Maturity

Mobile Device Management (MDM)

A scale from 1 - 9 referred to as Technology Readiness Levels (TRLs) was adopted by the Department of Defense as a method of estimating technology maturity during the acquisition process.

The following outlines the scale of TRLs with the associated description:
1. Basic principles observed and reported. - Lowest level of technology readiness. Scientific research begins to be translated into applied research and development. Examples might include paper studies of a technology's basic properties.

2. Technology concept and/or application formulated. Invention begins. Once basic principles are observed, practical applications can be invented. Applications are speculative and there may be no proof or detailed analysis to support the assumptions. Examples are limited to analytic studies.

3. Analytic and experimental critical function and/or characteristic proof of concept. Active research and development is initiated. This includes analytical studies and laboratory studies to physically validate analytical predictions of separate elements of the technology. Examples include components that are not yet integrated or representative.

4. Component and/or breadboard validation in laboratory environment. Basic technological components are integrated to establish that they will work together. This is relatively "low fidelity" compared to the eventual system. Examples include integration of "ad hoc" hardware in the laboratory.

5. Component and/or breadboard validation in relevant environment. Fidelity of breadboard technology increases significantly. The basic technological components are integrated with reasonably realistic supporting elements so it can be tested in a simulated environment. Examples include "high fidelity" laboratory integration of components.

6. System/subsystem model or prototype demonstration in a relevant environment. Representative model or prototype system, which is well beyond that of TRL 5, is tested in a relevant environment. Represents a major step up in a technology's demonstrated readiness. Examples include testing a prototype in a high-fidelity laboratory environment or in simulated operational environment.

7. System prototype demonstration in an operational environment. Prototype near, or at, planned operational system. Represents a major step up from TRL 6, requiring demonstration of an actual system prototype in an operational environment such as an aircraft, vehicle, or space. Examples include testing the prototype in a test bed aircraft.

8. Actual system completed and qualified through test and demonstration. Technology has been proven to work in its final form and under expected conditions. In almost all cases, this TRL represents the end of true system development. Examples include developmental test and evaluation of the system in its intended weapon system to determine if it meets design specifications.

9. Actual system proven through successful mission operations. Actual application of the technology in its final form and under mission conditions, such as those encountered in operational test and evaluation. Examples include using the system under operational mission conditions.

Mobile Device Management (MDM)

26. What TRL most accurately describes MDM systems?

- 1 - Basic principles observed and reported
- 2 - Technology concept and/or application formulate
- 3 - Analytic and experimental critical function and/or characteristic proof of concept
- 4 - Component and/or breadboard validation in laboratory environment
- 5 - Component and/or breadboard validation in relevant environment
- 6 - System/subsystem model or prototype demonstration in a relevant environment
- 7 - System prototype demonstration in an operational environment
- 8 - Actual system completed and qualified through test and demonstration
- 9 - Actual system proven through successful mission operations

Other (please specify)

MDM - Part 3 In Depth Questionnaire

Part 3

- is an In Depth Questionnaire intended for you to provide as much or as little information as you choose.

- will allow you to expound on concepts or issues not addressed previously.

We encourage you to browse questions. You are able to respond in any order at your convenience.

Thank you again for your time and service.

MDM - Operational Experience

The following questions deals with your experience in the deployment, integration, management and or operational usage, of a MDM system.

27. Have you experience in the deployment, integration, management and or operational usage, of a MDM system?

- Yes
- No

MDM - Operational Experience Questionnaire

Mobile Device Management (MDM)

28. How has the capability of the MDM system influenced your TTPs in current operations? (please specify)

29. Can you comment on any systematic issues or concerns with the system possibly including, but not limited to, Information Assurance or how the managed devices are operating/functioning.

30. What operational capabilities does the MDM system bring to your unit / agency / organization?

31. Has the MDM system changed the way your unit operates?

32. What operational options does the MDM system bring to your unit?

33. List operational strengths of the system.

34. List operational weakness or limitations of the system.

35. What significant operational considerations should other Information or Acquisition professionals keep in mind when planning to deploy, employ, or manage a MDM system?

Mobile Device Management (MDM)

36. How has the system been used most effectively?

37. In what ways has the system not been effective?

MDM - Critical Technology Elements

In the following questions, we are attempting to gather your opinion on Critical Technology Elements (CTEs) associated with MDM systems.

CTEs can be hardware or software. The definition of a CTE is as follows:
A technology element is "critical" if the system being acquired depends on this technology element to meet operational requirements (within acceptable cost and schedule limits)

and

if the technology element or its application is either new or novel or in an area that poses major technological risk during detailed design or demonstration.

38. What would you propose would meet the definition of a CTE in regards to MDM?

39. How is the commercial use of this CTE different from the DoD use?

40. Will this CTE work in large-scale environments such as the DoD GIG?

41. What aspects of the system design are dependent on unique features or particular versions of the CTE?

Mobile Device Management (MDM)

42. Will this CTE be modified, tailored, extended, or enhanced from its original state?

43. Does this CTE depend on other systems?

44. In reference to terminal hardware - Are there extenuating physical environment considerations for size, weight, visibility in daylight, or usability?

Terminal hardware consists of video displays, audio/ sound systems, keyboards, touch-screen terminals, personal digital assistants (PDAs) and so forth.

45. In reference to Processing Hardware - Are needed software development environments supported?

Processing hardware consists of processors, memory, servers, supercomputers, mainframes, blade servers (self-contained, all-inclusive computer servers with a design optimized to minimize physical space), and so forth.

46. In reference to Processing Hardware - Have any significant changes been made or required for the operating system and other systems software?

Processing hardware consists of processors, memory, servers, supercomputers, mainframes, blade servers (self-contained, all-inclusive computer servers with a design optimized to minimize physical space), and so forth.

Mobile Device Management (MDM)

47. In reference to Networking - Is the topology (logical and hardware) new? Do the peak and average data rates require new hardware or algorithms in the system?

Networking hardware consists of routers, switches, access points, network interface cards (NICs), local area network/wide area network (LAN/WAN) components, storage area network (SAN) components,
and so forth.

48. In reference to Networking - Do requirements for bandwidth, delay, jitter, loss, and availability imply that new or modified hardware is required?

Networking hardware consists of routers, switches, access points, network interface cards (NICs), local area network/wide area network (LAN/WAN) components, storage area network (SAN) components,
and so forth.

49. In reference to Networking - Have the wireless devices been used previously in the anticipated electromagnetic environment?

Networking hardware consists of routers, switches, access points, network interface cards (NICs), local area network/wide area network (LAN/WAN) components, storage area network (SAN) components,
and so forth.

Mobile Device Management (MDM)

50. In reference to Networking - Is wireless performance acceptable and or available in the expected electromagnetic environment?

Networking hardware consists of routers, switches, access points, network interface cards (NICs), local area network/wide area network (LAN/WAN) components, storage area network (SAN) components,
and so forth.

51. In reference to Networking - Is the network hardware able to grow in physical size and bandwidth while still satisfying key performance requirements?

Networking hardware consists of routers, switches, access points, network interface cards (NICs), local area network/wide area network (LAN/WAN) components, storage area network (SAN) components,
and so forth.

52. How do issues of scalability affect a MDM product?

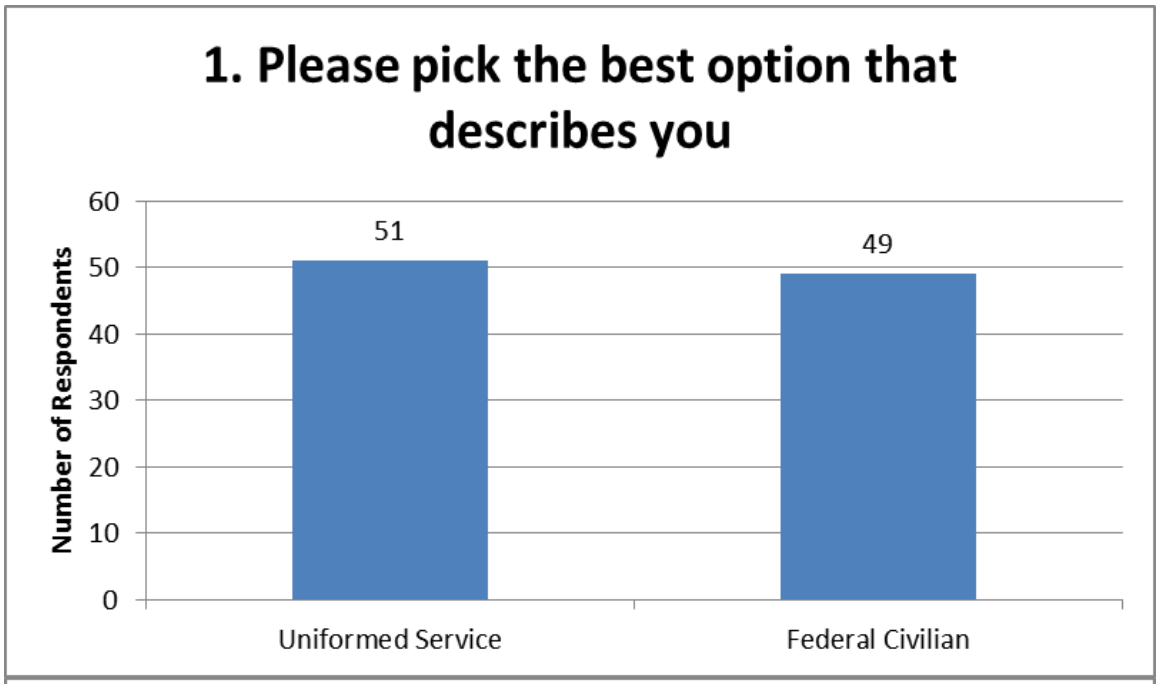
53. Have MDM products been run in organizations that have similar numbers of users, similar sizes of data sets, and similar suites of applications?

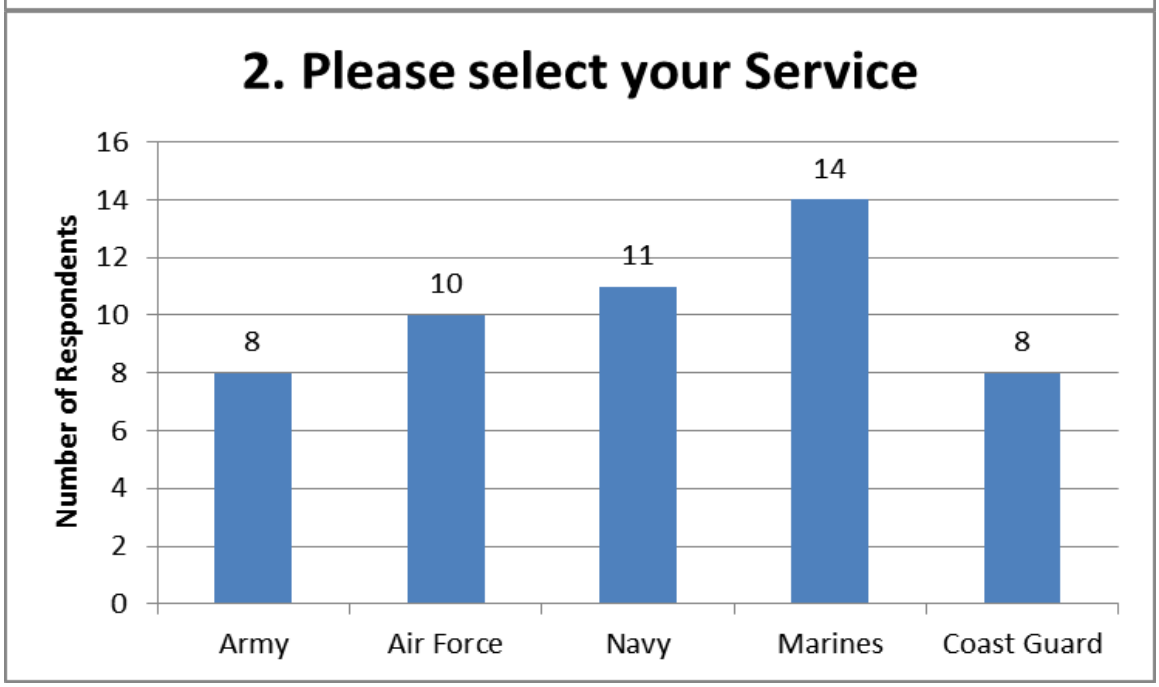
54. Do you believe that one system is scalable commensurate with its anticipated use in DoD? Is that scalability affected by any other chosen technologies (e.g., IA)?

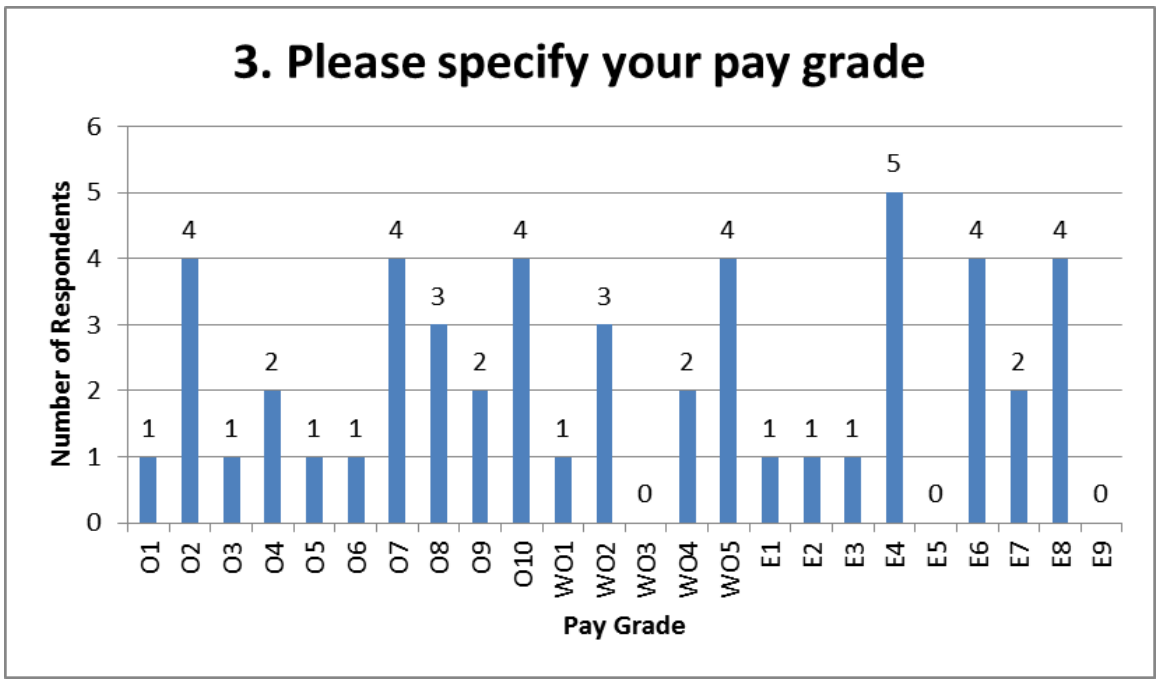
55. How does the DoD environment differ from the environments in which the components have been used previously?

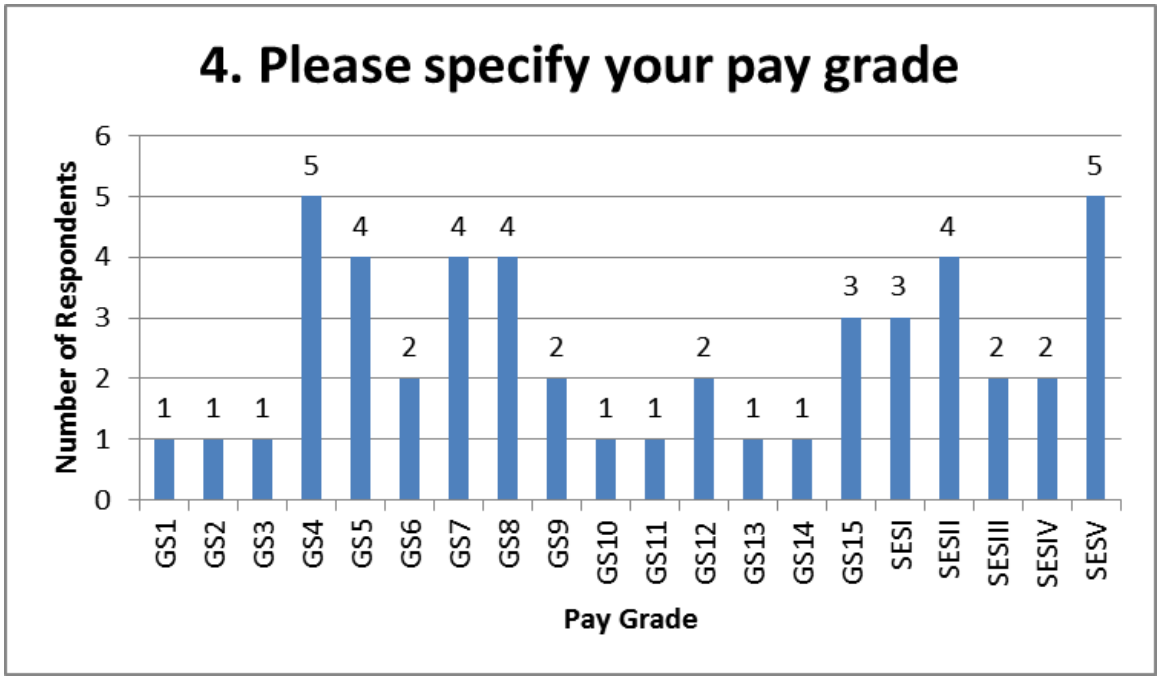
THIS PAGE INTENTIONALLY LEFT BLANK

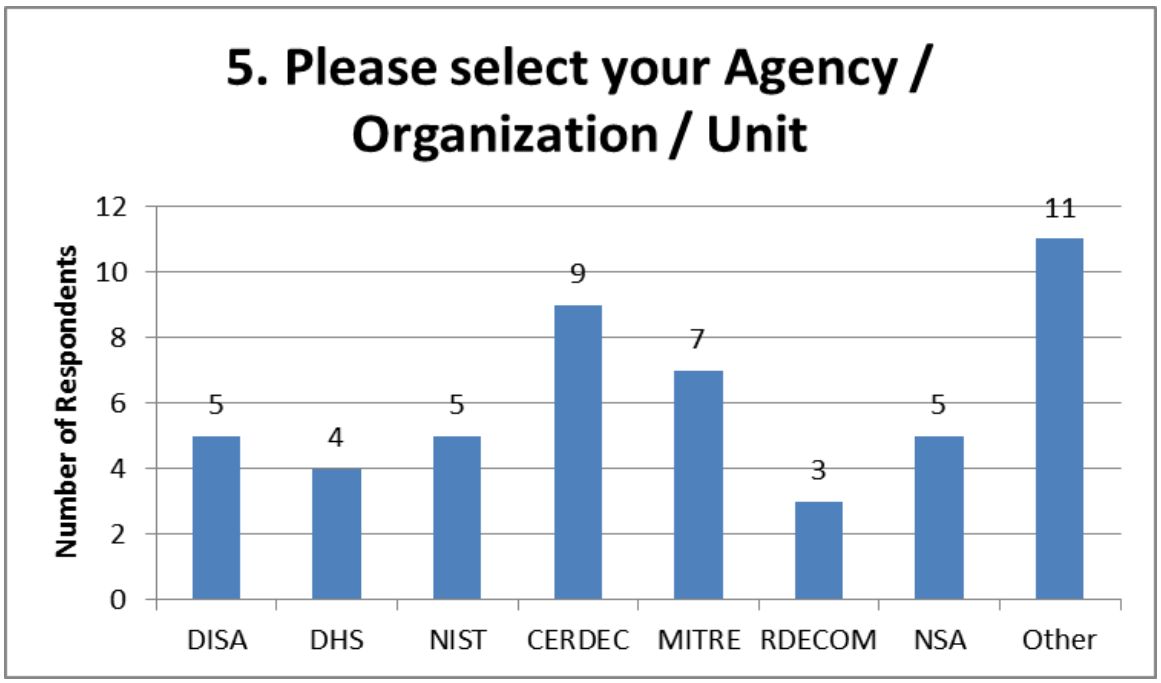
APPENDIX J. EXAMPLE SURVEY RESULTS

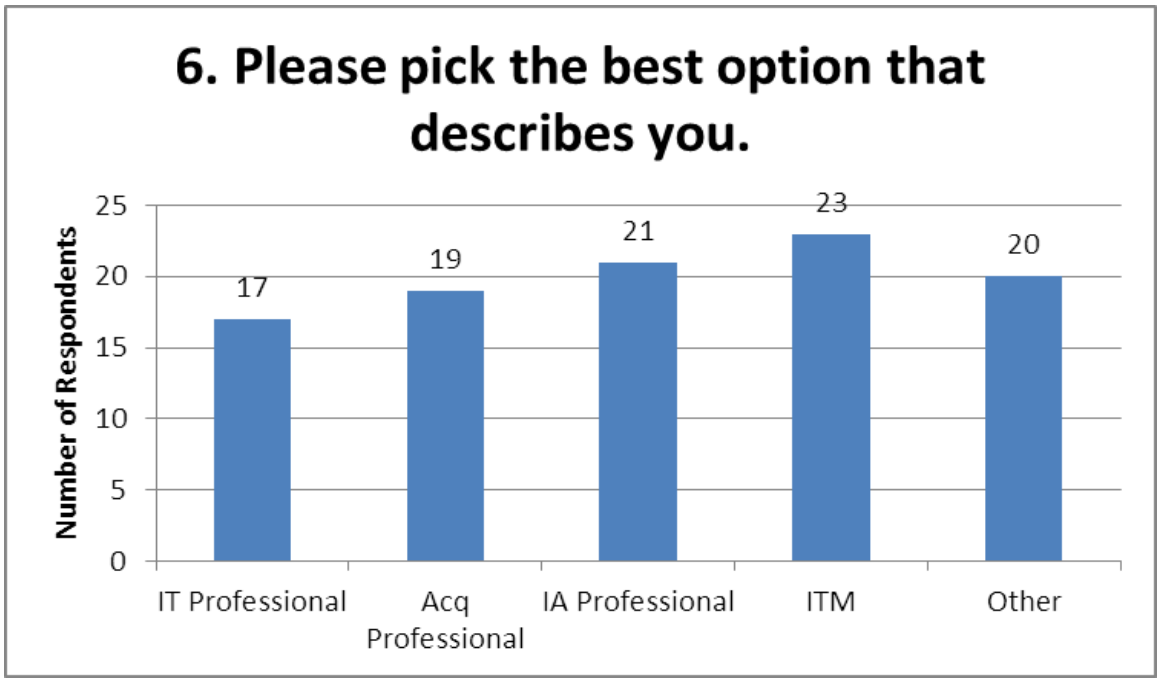


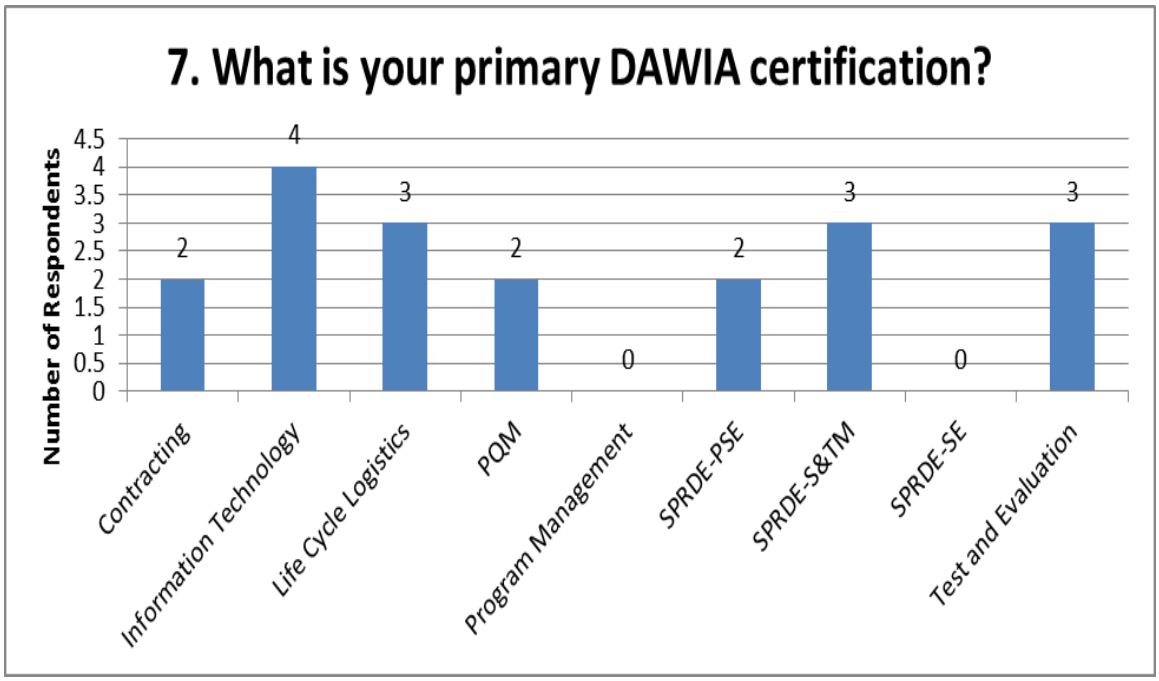


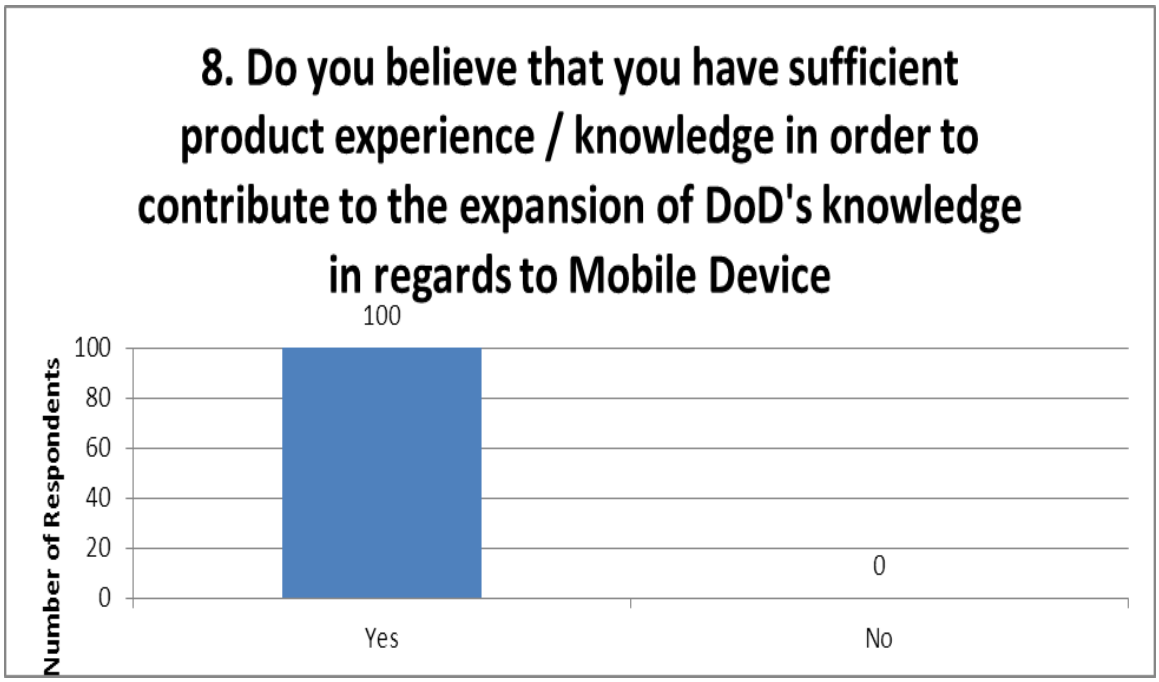

3. Please specify your pay grade
Number of Respondents
0
1
2
3
4
5
6
1
4
1
2
1
1
4
3
2
4
1
3
0
2
4
1
1
1
5
0
4
2
4
0
O1
O2
O3
O4
O5
O6
O7
O8
O9
O10
WO1
WO2
WO3
WO4
WO5
E1
E2
E3
E4
E5
E6
E7
E8
E9
Pay Grade

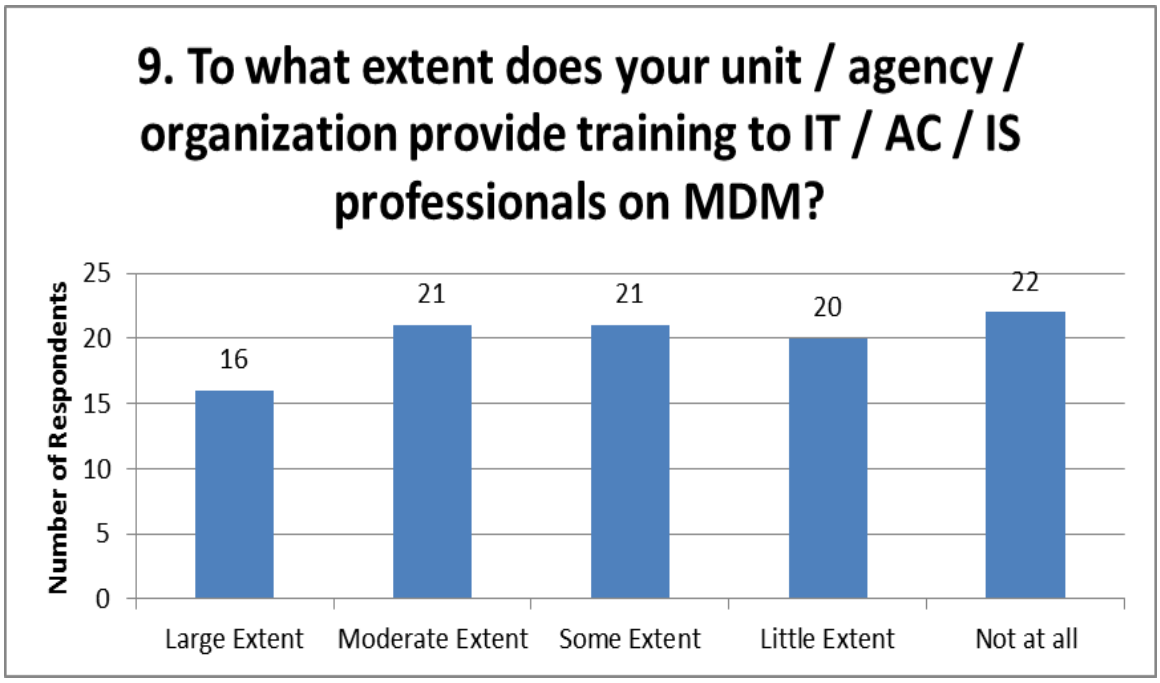

4. Please specify your pay grade
Number of Respondents
0
1
2
3
4
5
6
1
1
1
5
4
2
4
4
2
1
1
2
1
1
3
3
4
2
2
5
GS1
GS2
GS3
GS4
GS5
GS6
GS7
GS8
GS9
GS10
GS11
GS12
GS13
GS14
GS15
SESI
SESII
SESIII
SESIV
SESV
Pay Grade

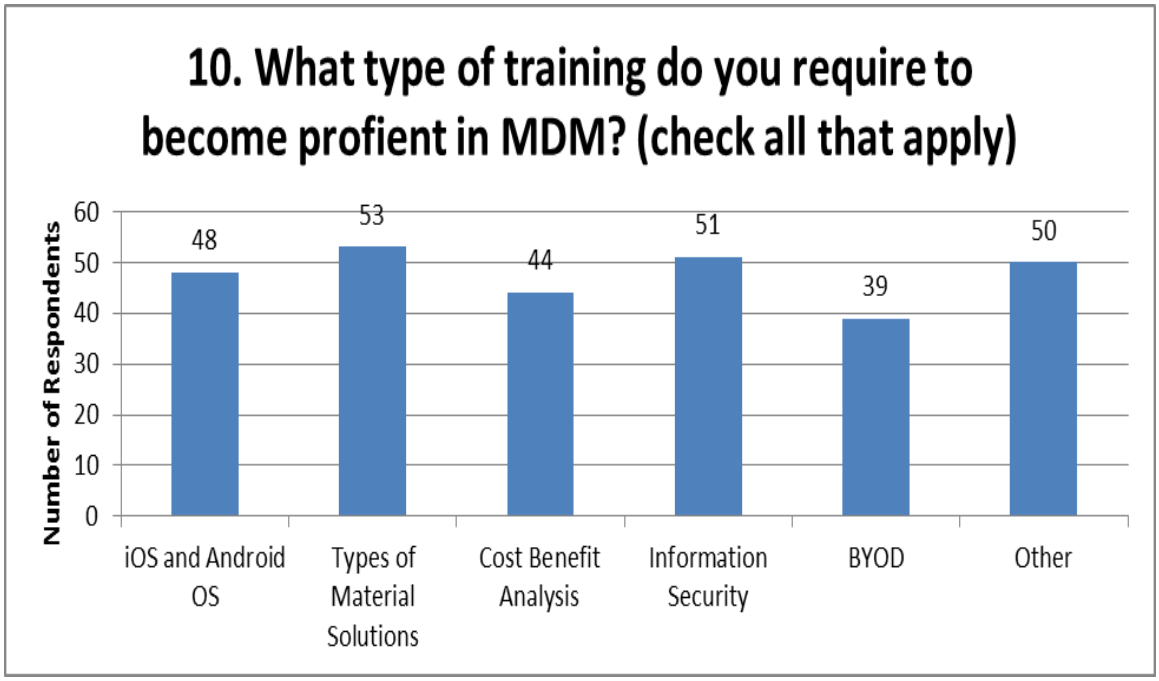

5. Please select your Agency / Organization / Unit
Number of Respondents
0
2
4
6
8
10
12
5
4
5
9
7
3
5
11
DISA
DHS
NIST
CERDEC
MITRE
RDECOM
NSA
Other


6. Please pick the best option that describes you.
Number of Respondents
0
5
10
15
20
25
17
19
21
23
20
IT Professional
Acq Professional
IA Professional
ITM
Other

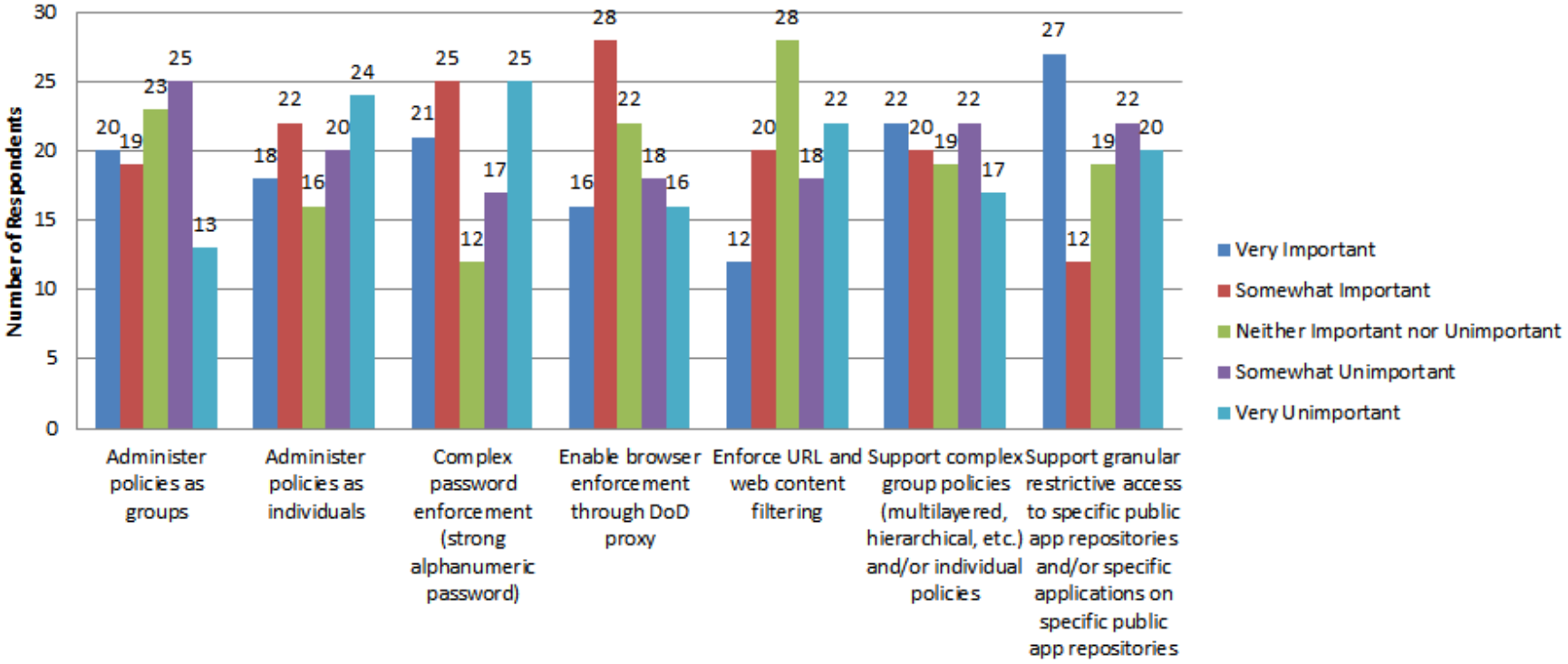

7. What is your primary DAWIA certification?
Number of Respondents
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
2
4
3
2
0
2
3
0
3
Contracting
Information Technology
Life Cycle Logistics
PQM
Program Management
SPRDE-PSE
SPRDE-S&TM
SPRDE-SE
Test and Evaluation


8. Do you believe that you have sufficient product experience / knowledge in order to contribute to the expansion of DoD's knowledge in regards to Mobile Device
Number of Respondents
100
80
60
40
20
0
100
0
Yes
No

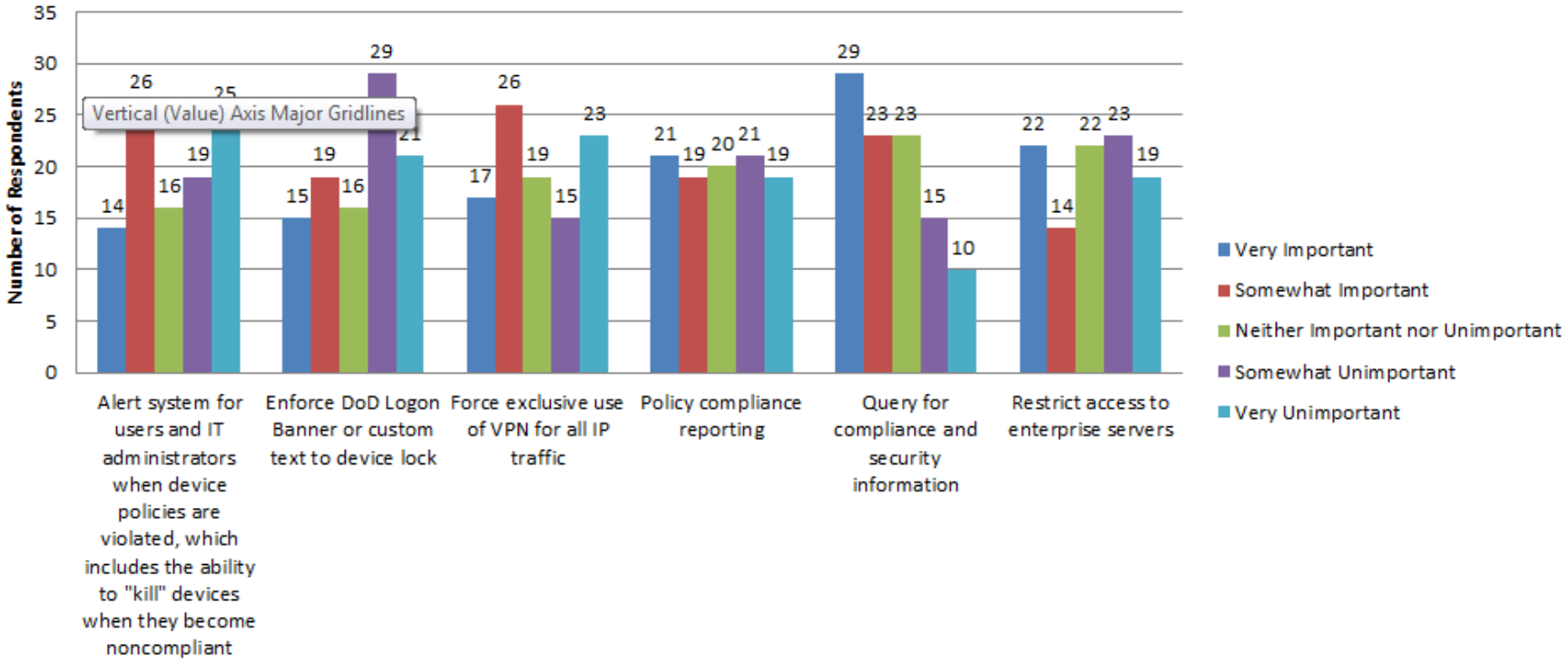

9. To what extent does your unit / agency / organization provide training to IT / AC / IS professionals on MDM?
Number of Respondents
25
20
15
10
5
0
16
21
21
20
22
Large Extent
Moderate Extent
Some Extent
Little Extent
Not at all


10. What type of training do you require to become profient in MDM? (check all that apply)
Number of Respondents
60
50
40
30
20
10
0
48
53
44
51
39
50
iOS and Android OS
Types of Material Solutions
Cost Benefit Analysis
Information Security
BYOD
Other

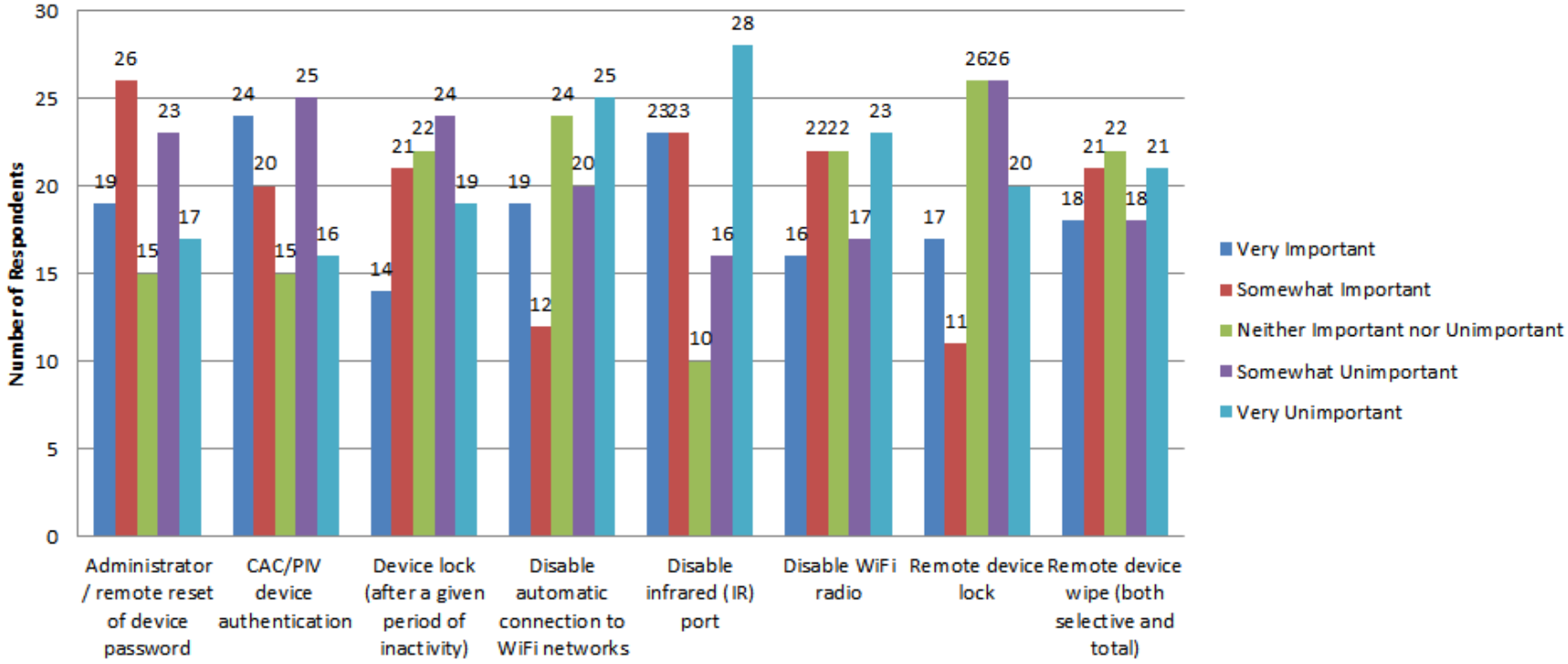
11. How important are the following attributes for Policy Management to MDM:



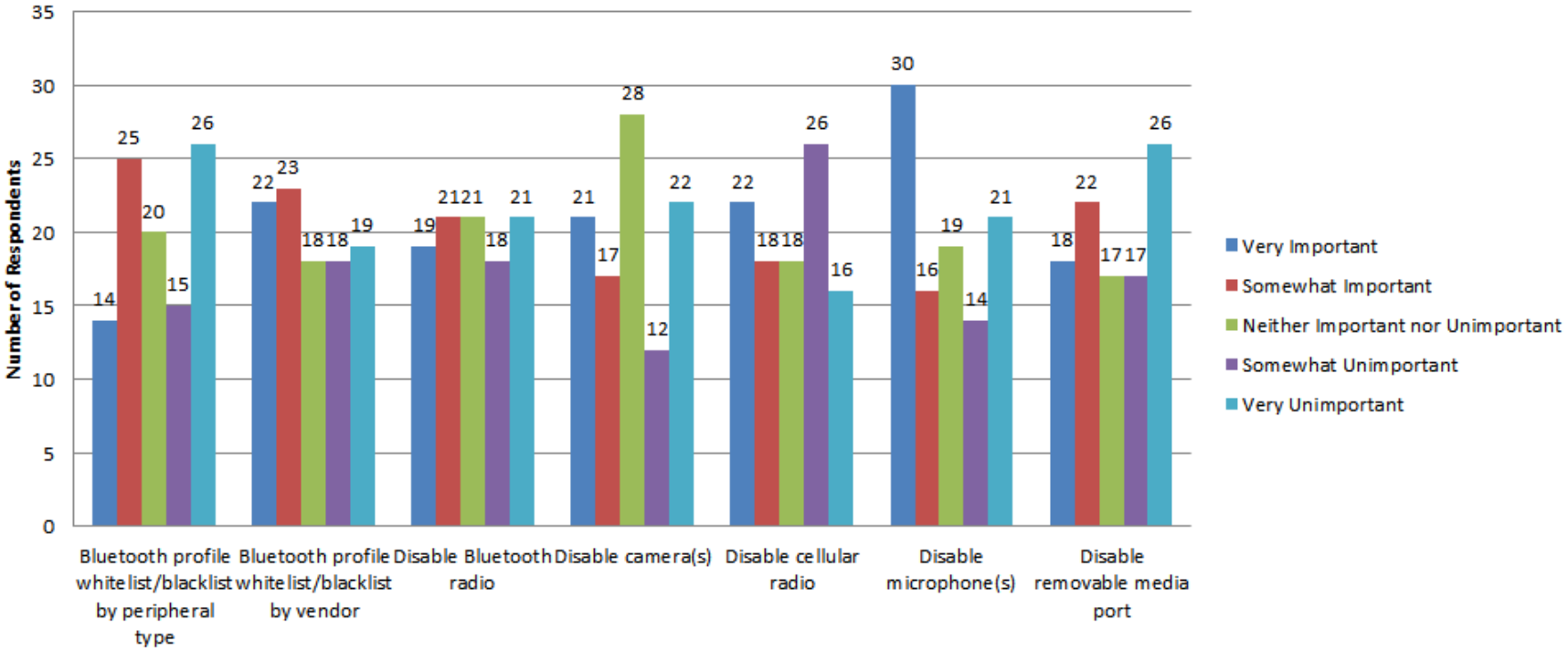
12. How important are the following atrributes for Policy Management to MDM:



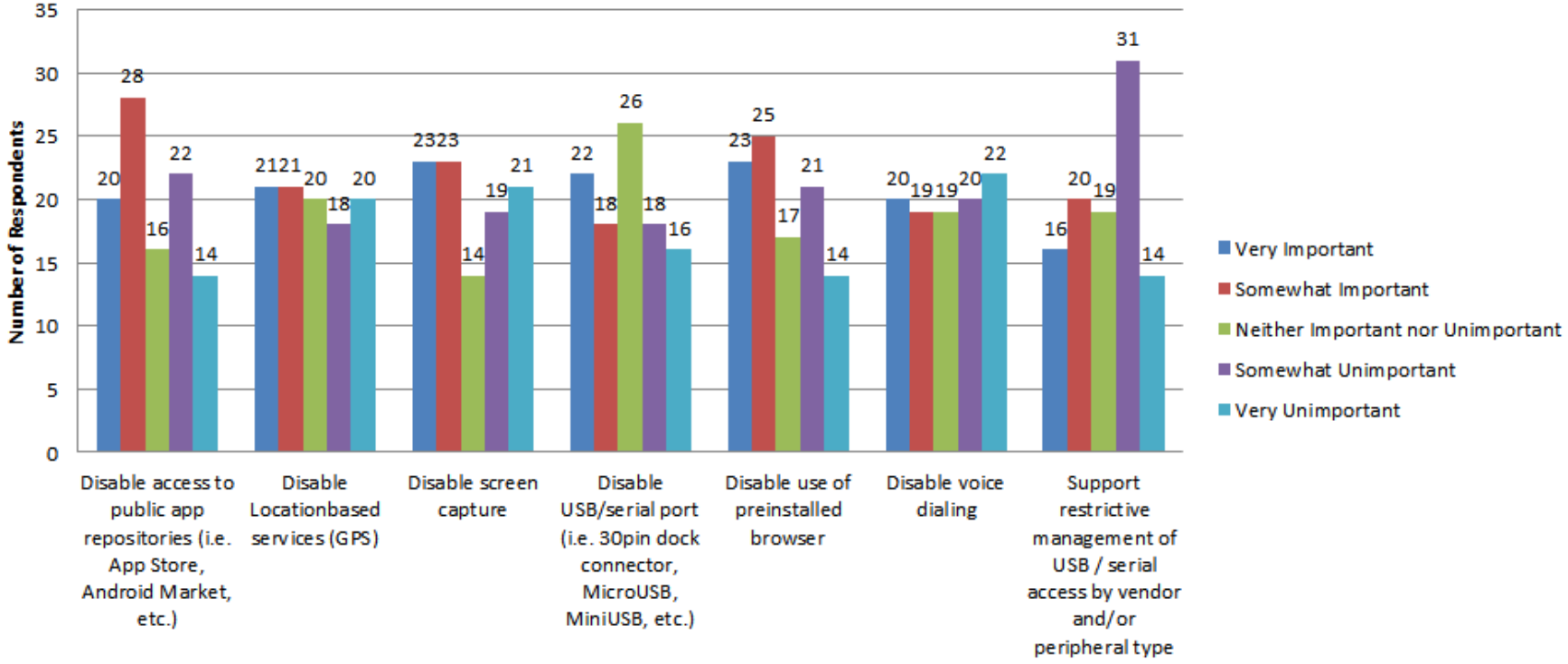
13. How important are following attributes for Security Management to MDM:



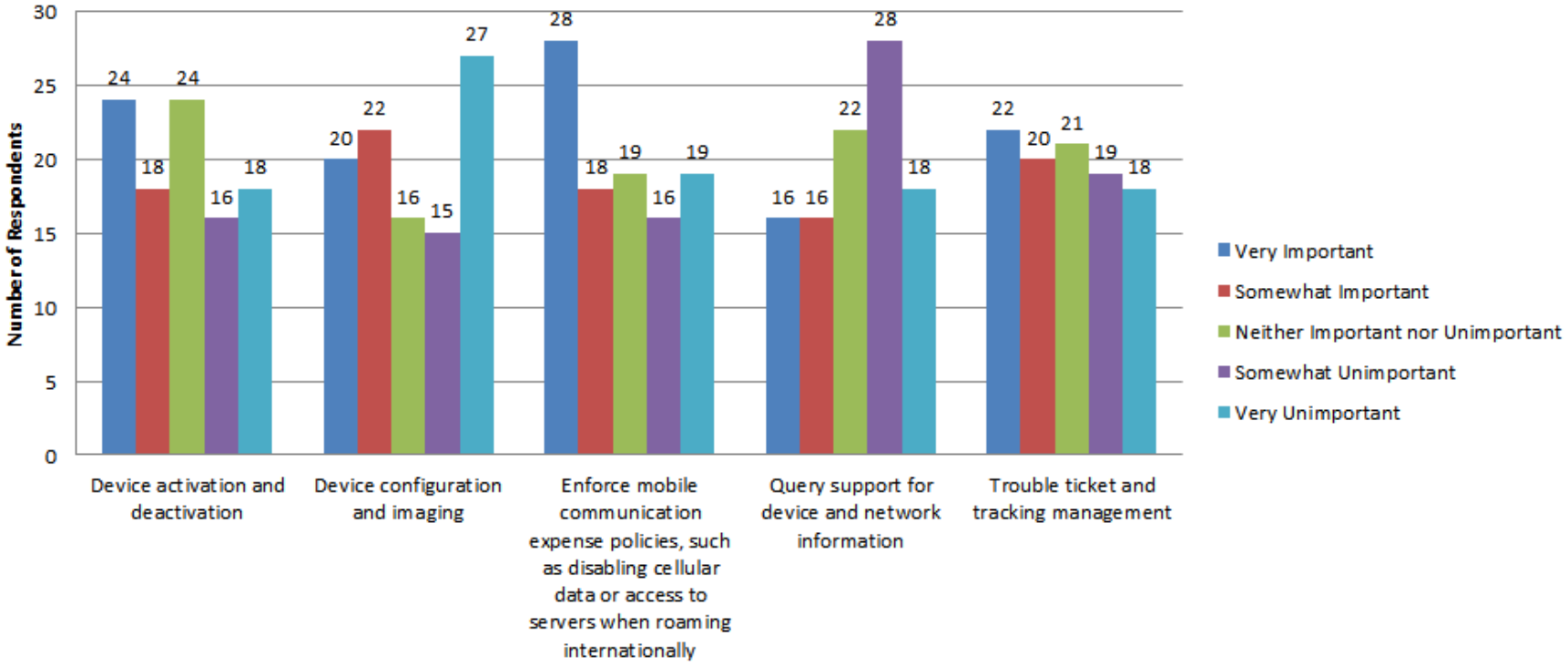
14. How important are following attributes for Security Management to MDM:



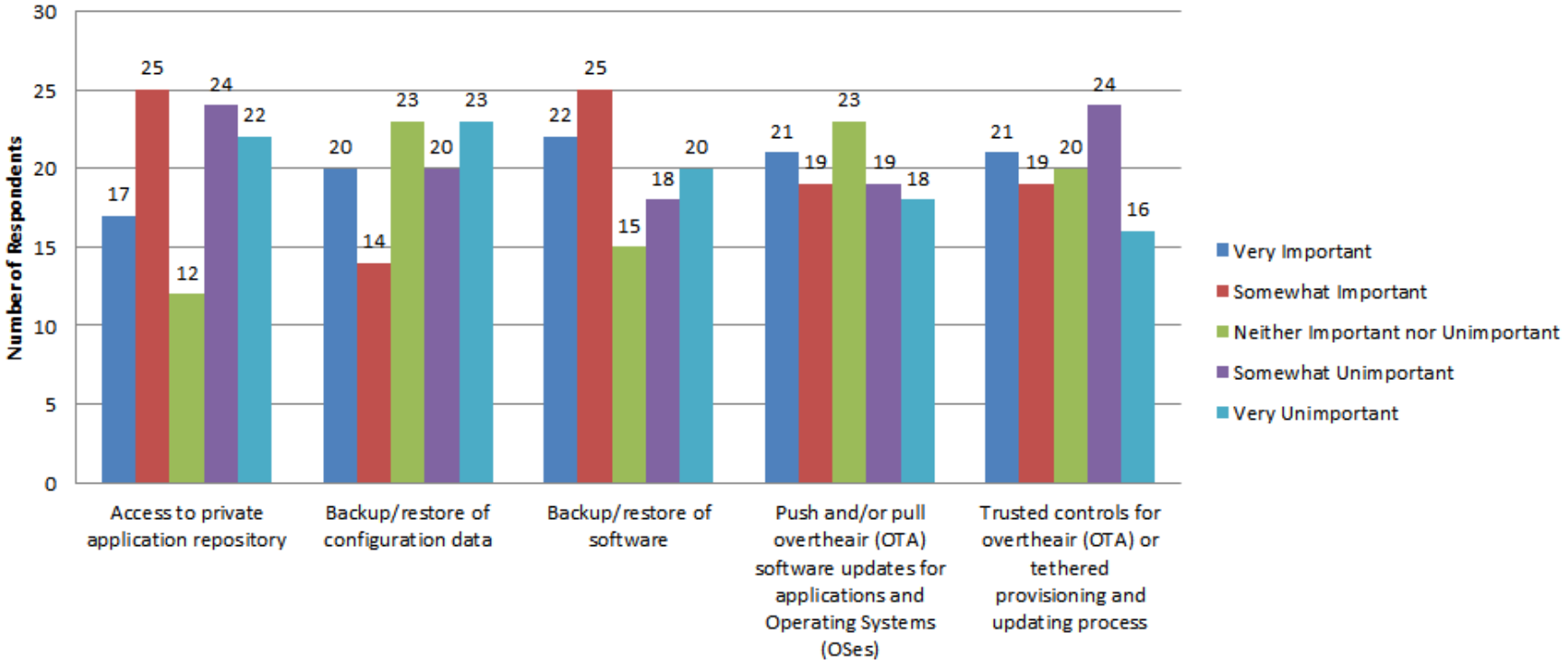
15. How important are following attributes for Security Management to MDM:

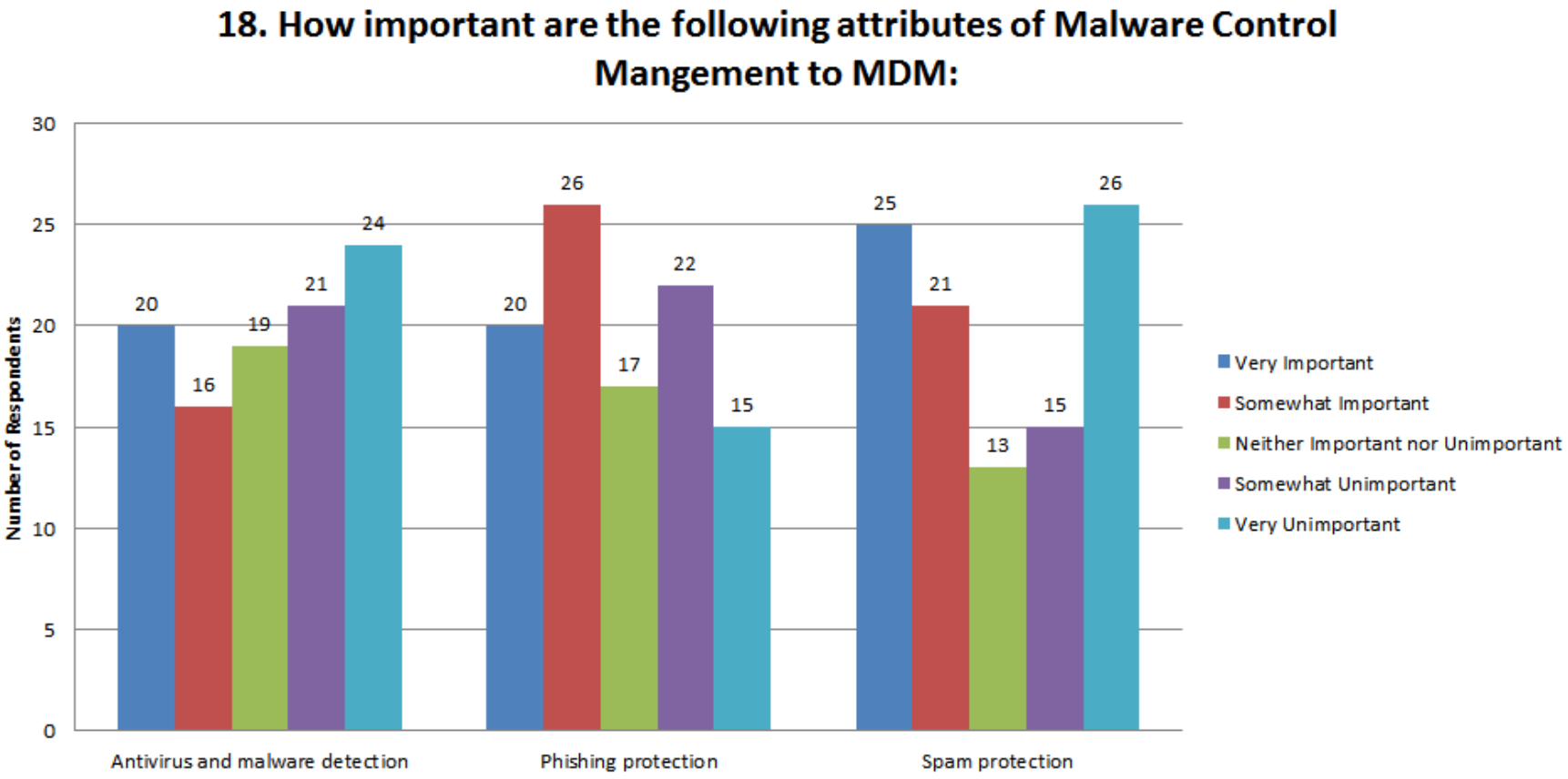


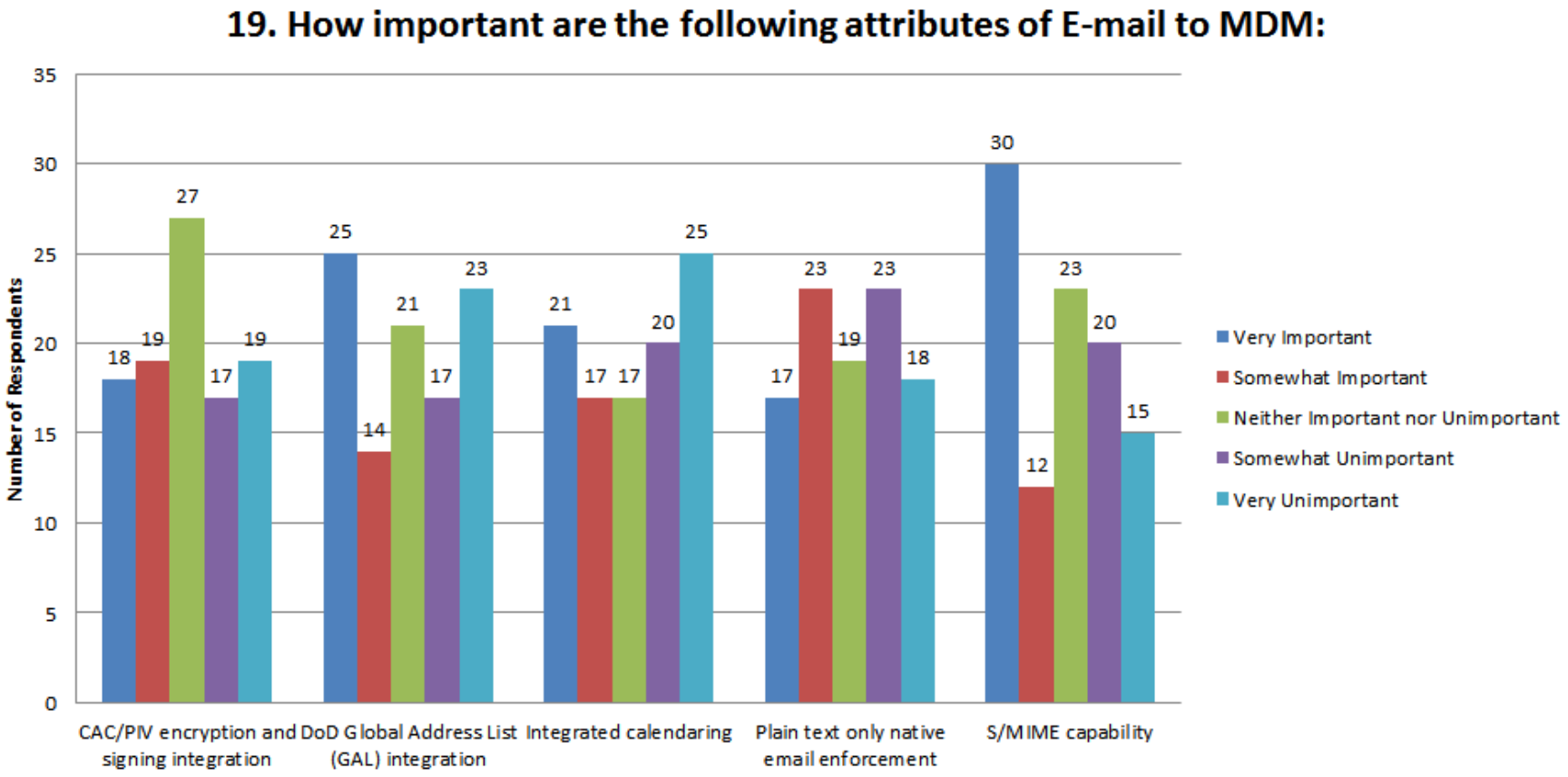
16. How important are the following attributes of Inventory Management to MDM:



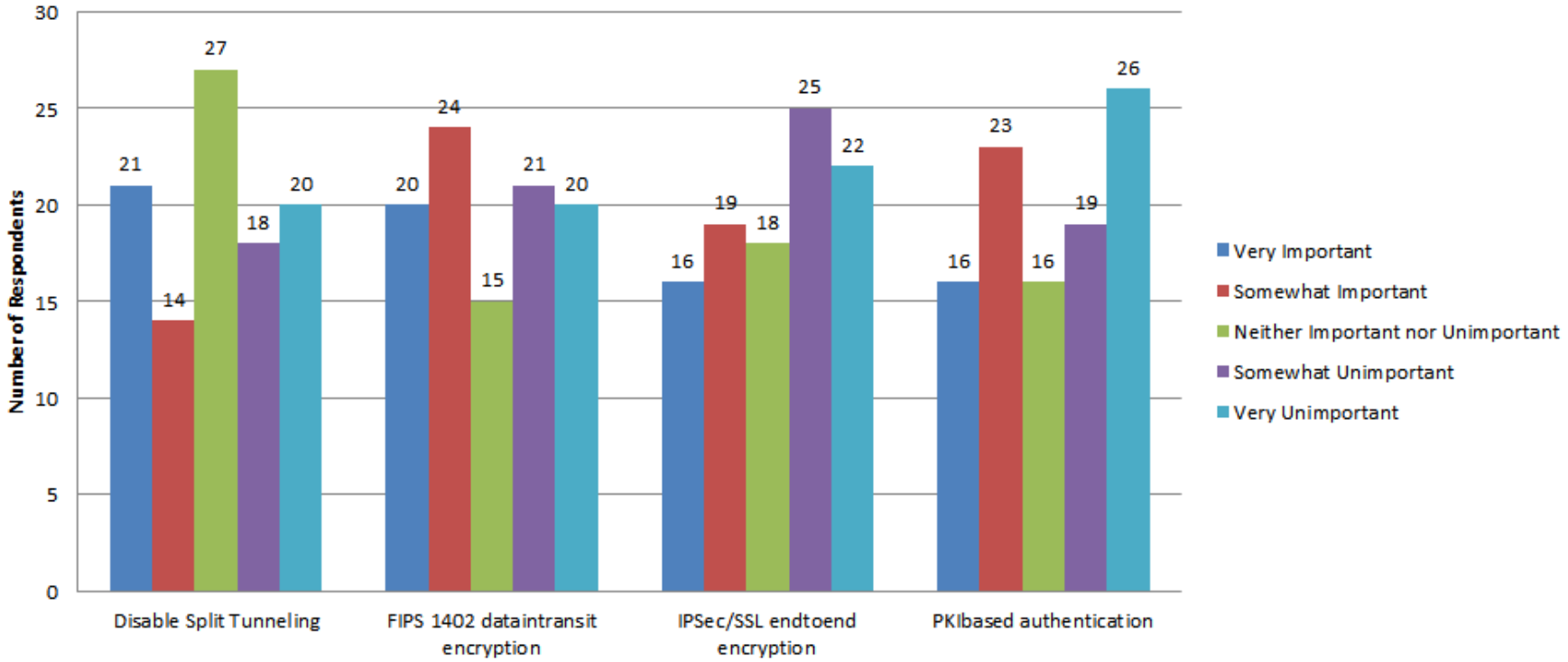
17. How important are the following attributes of Software Distribution to MDM:



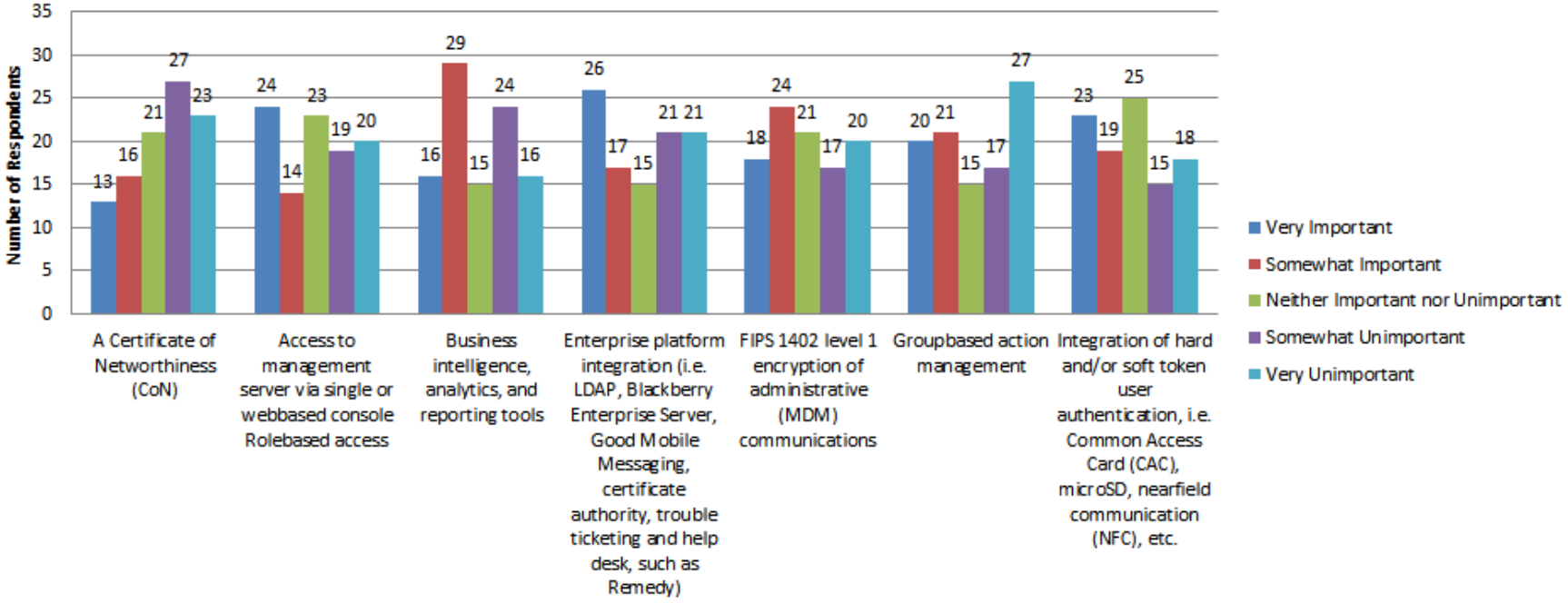

18. How important are the following attributes of Malware Control Mangement to MDM:
Number of Respondents
30
25
20
15
10
5
0
20
16
19
21
24
20
26
17
22
15
25
21
13
15
26
Antivirus and malware detection
Phishing protection
Spam protection
Very Important
Somewhat Important
Neither Important nor Unimportant
Somewhat Unimportant
Very Unimportant

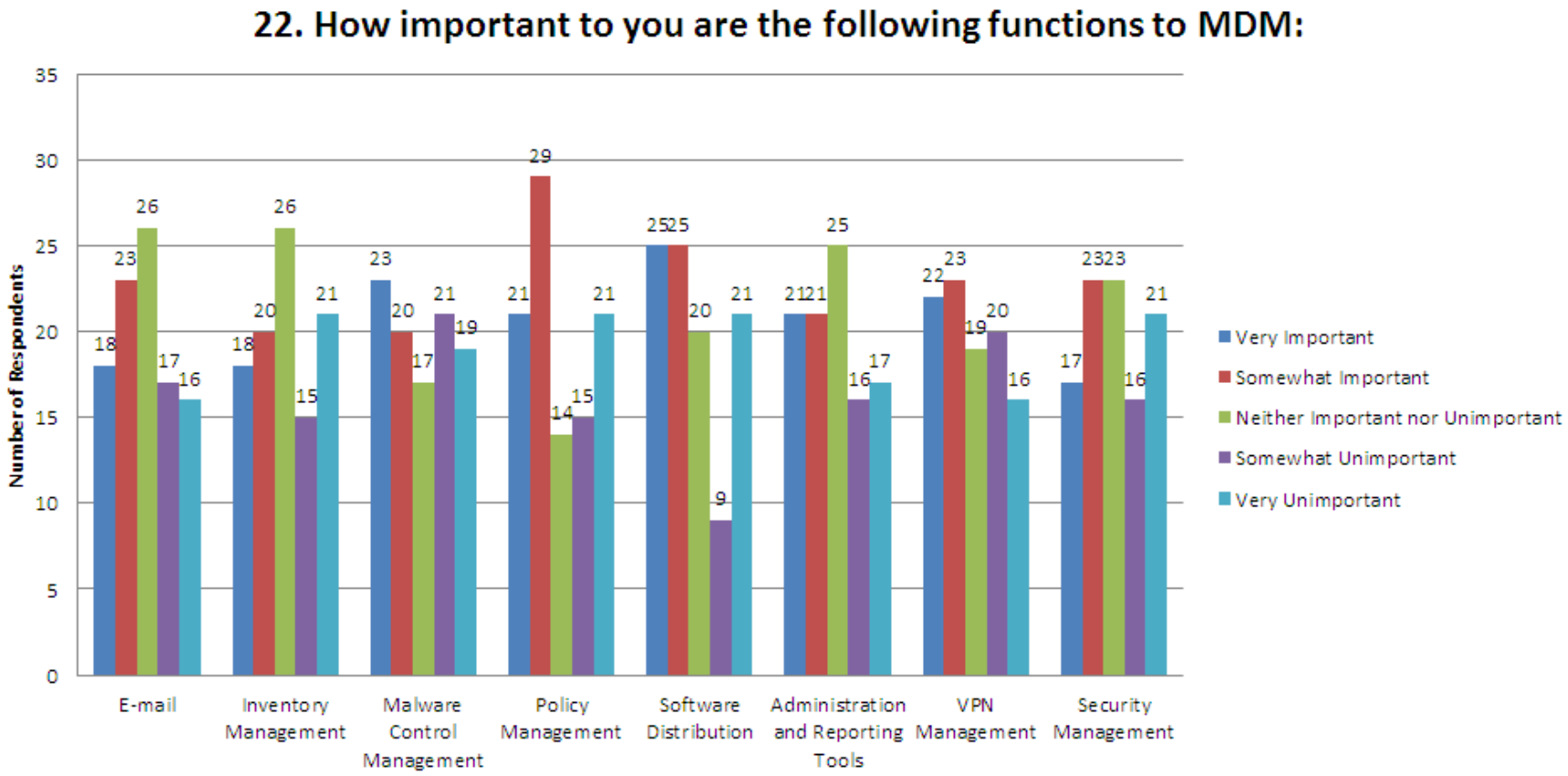

19. How important are the following attributes of E-mail to MDM:
Number of Respondents
35
30
25
20
15
10
5
0
18
19
27
17
19
25
14
21
17
23
21
17
17
20
25
17
23
19
23
18
30
12
23
20
15
CAC/PIV encryption and signing integration
DoD Global Address List (GAL) integration
Integrated calendaring
Plain text only native email enforcement
S/MIME capability
Very Important
Somewhat Important
Neither Important nor Unimportant
Somewhat Unimportant
Very Unimportant

20. How important are the following attributes of VPN Management to MDM:

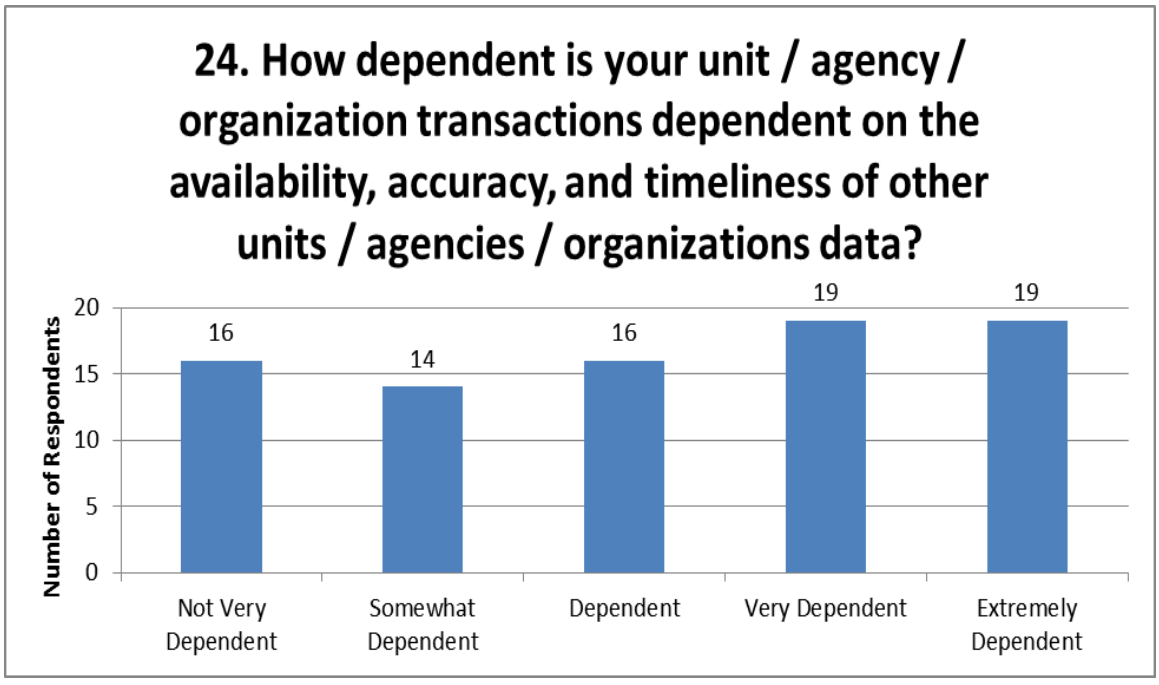


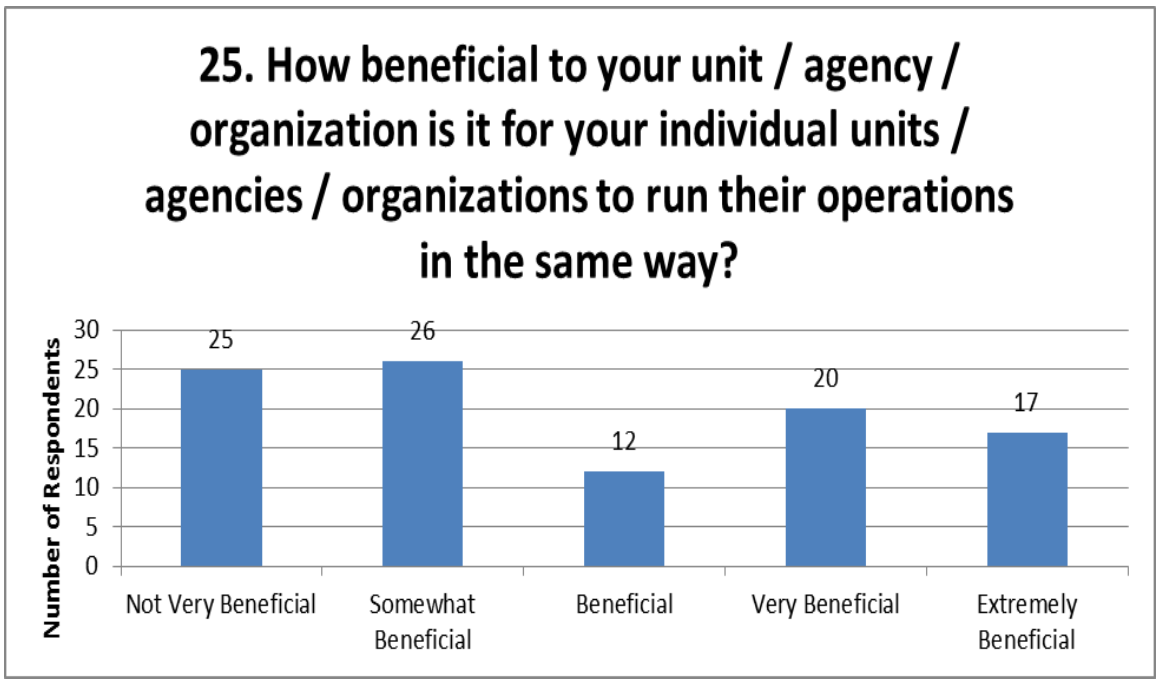
21. How important are the following attributes of Administration and Reporting Tools to MDM:

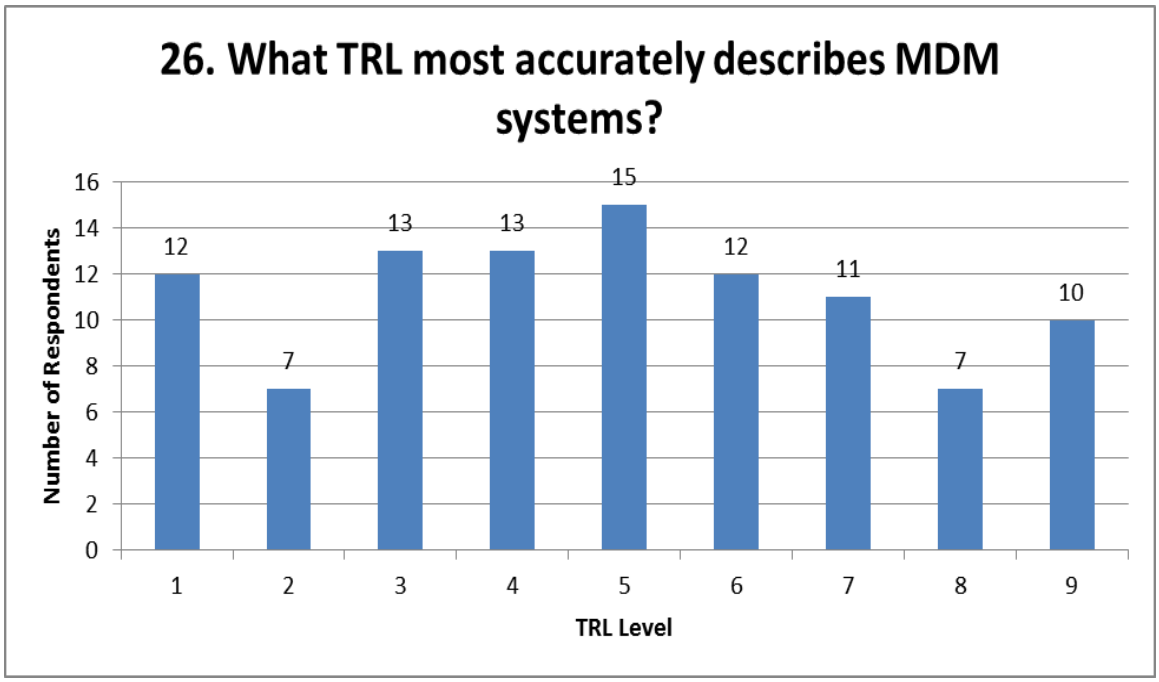



22. How important to you are the following functions to MDM:
Number of Respondents
35
30
25
20
15
10
5
0
E-mail
Inventory Management
Malware Control Management
Policy Management
Software Distribution
Administration and Reporting Tools
VPN Management
Security Management
Very Important
Somewhat Important
Neither Important nor Unimportant
Somewhat Unimportant
Very Unimportant


23. What best describes your organization's operating model:
Number of Respondents
35
30
25
20
15
10
5
0
25
18
32
25
Coordination
Unification
Diversification
Replication


24. How dependent is your unit / agency / organization transactions dependent on the availability, accuracy, and timeliness of other units / agencies / organizations data?
Number of Respondents
20
15
10
5
0
16
14
16
19
19
Not Very Dependent
Somewhat Dependent
Dependent
Very Dependent
Extremely Dependent


25. How beneficial to your unit / agency / organization is it for your individual units / agencies / organizations to run their operations in the same way?
Number of Respondents
30
25
20
15
10
5
0
25
26
12
20
17
Not Very Beneficial
Somewhat Beneficial
Beneficial
Very Beneficial
Extremely Beneficial


26. What TRL most accurately describes MDM systems?
Number of Respondents
16
14
12
10
8
6
4
2
0
12
7
13
13
15
12
11
7
10
1
2
3
4
5
6
7
8
9
TRL Level

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX K. RESPONDENT NOTIFICATION

To: [e-mail]
From: [insert e-mail here]

Subject: [insert Institutional / Organizational name here] Mobile Device Management Survey
Body: Dear [insert Title and Name here],

My name is [insert Name here]. I am assigned to the [insert Institutional / Organizational name here] in [insert City, State] conducting research in support of a master's level thesis. The Principal Investigator is [insert Name, position, and contact information here]. The Institutional Review Board Chair is [insert Name and contact information here].

I am contacting Subject Matter Experts in the fields of Information Systems, Information Assurance, and Department of Defense (DoD) Acquisitions in order to expand the body of knowledge for Mobile Device Management. I feel that your understanding and experience would benefit the DoD community at large and contribute greatly to my research.

The title of my thesis is [insert ThesisName here]. I am gathering data in order to analyze the current use and management of mobile devices on the DoD network, the risk factors present, integration issues encountered, and future plans for mobile device management. I feel my end product will capture the concerns of IT professionals and provide acquisitions professionals with a better understanding of factors for analysis when acquiring mobile device management solutions.

I would appreciate your support in my research through participation in a web survey.

Here is a link to the survey:
[insert web link here]

This link is uniquely tied to this survey and your e-mail address. Please do not forward this message.

Please note: If you do not wish to receive further e-mails from me, please click the link below, and you will be automatically removed from my mailing list.
[insert web link here]

Thank you for your help, support, and service. My contact information is provided below.

Very respectfully
[insert Name here]

[insert signature block here]

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ackermann, F., & Eden, C. (2011). Strategic management of stakeholders: Theory and practice. *Long Range Planning*, *44*(3), 179–196.

Apple. (2012). *iPhone and iPad in business deployment scenarios*. Retrieved from http://images.apple.com/ipad/business/docs/iOS_6_Business_Sep12.pdf

Army Contracting Command. (2011). Request for information (RFI) for Program Management Network and Enterprise Services (PM NES) establishment of mobile device management services (Solicitation number W91WAWPMNES2). Retrieved from https://www.fbo.gov/index?id=540603238a568a19e106a8b59b7df7d6

Avema Critical Wireless. (2011). What is bring your own device (BYOD)? Retrieved from http://www.avema.com/mobile_device_management_blog/byod/what-is-bring-your-own-device-byod/

Banker, R. D., Hu, N., Pavlou, P. A., & Luftman, J. (2011). CIO reporting structure, strategic positioning, and firm performance. *MIS Quarterly*, *35*(2), 487–504.

Bologa, C., Faur, G., & Ghisoiu, N. (2010). Generic model of an enterprise information architecture for a public institution. *Journal of Computer Science and Control Systems, 3*(1).

Boyles, J. L., Smith, A., & Madden, M. (2012). *Privacy and data management on mobile devices.* Retrieved from Pew Internet & American Life Project website: http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx

Burt, J. (2011). BYOD trend pressures corporate networks. *eWeek, 28*(14), 30–31. Retrieved from http://84.201.93.40/images/2/2e/65469365.pdf

Chen, D. Q., Preston, D. S., & Xia, W. (2010). Antecedents and effects of CIO supply-side and demand-side leadership: A staged maturity model. *Journal of Management Information Systems*, *27*(1), 231–271.

Clinger–Cohen Act of 1996, Pub. L. No. 104–106, § Sec. 5125 110 Stat. 642 (1996).

Communications-Electronics Research, Development, and Engineering Center (CERDEC). (2013). About CERDEC. Retrieved from http://www.cerdec.army.mil/about/index.asp

Creswell, J., & Clark, V. (2006). *Designing and conducting mixed methods research.* Thousand Oaks, CA: Sage.

Dawson, G. S., & Kauffman, R. J. (2010, January). *Are CIOs any different? Analyzing the job tenures of C-suite executives in the public sector*. Paper presented at the 43rd Hawaiian International Conference on System Sciences (HICSS), Kauai, HI.

Dean, T. (2010). *Network+ guide to networks* (5th ed.). Boston, MA: Course Technology.

Defense Acquisition University (DAU). (2012). *Featured - Life Cycle Framework*. Retrieved from https://dap.dau.mil/aphome/das/Pages/Default.aspx

Defense Acquisition University (DAU). (2013). *Acquisition, technology & logistics workforce position category descriptions (PCDs).* Retrieved from http://www.dau.mil/workforce/pages/pcds.aspx

Defense Acquisition Workforce Improvement Act (DAWIA) of 1990, 10 U.S.C § 1701 (1990).

Defense Business Board. (2012). *DoD information technology modernization: A recommended approach to data center consolidation and cloud computing*. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA556335

Defense Information Systems Agency (DISA). (2013). About DISA. Retrieved from http://www.disa.mil/About/Our-Work

Department of Defense (DoD). (2010). DoDAF Architecture Framework (Ver. 2.02). Washington, DC: Author.

Department of Defense (DoD) Chief Information Officer (CIO). (2012). Department of Defense mobile device strategy (Ver. 2.0). Washington, DC: Author.

Department of Defense (DoD) Systems Management College. (2001). *System engineering fundamentals*. Fort Belvoir, VA: Defense Acquisition University Press.

Digital Service Advisory Group & Federal Chief Information Officer's Council. (2012). *Government use of mobile technology: Barriers, opportunities, and gap analysis*. Retrieved from https://cio.gov/wp-content/uploads/downloads/2012/12/Government_Mobile_Technology_Barriers_Opportunities_and_Gaps.pdf

Dillard, J., & Ford, D. (2009). From amorphous to defined: Balancing risks in evolutionary acquisition. *Defense Acquisitions Research Journal, 16 (3*) P 234–256. Retrieved from http://www.dau.mil/pubscats/PubsCats/Dillard.pdf

Director, Research Directorate, Office of the Director, Defense Research and Engineering (DRD DDR&E). (2009). *Technology Readiness Assessment (TRA) deskbook.* Washington, DC: Department of Defense.

Durmusoglu, S. S. (2009). The role of top management team's information technology (IT) infrastructure view on new product development. *European Journal of Innovation Management, 12*(3), 364–385.

Englander, I. (2009). *The architecture of computer hardware, system software, and networking* (4th ed.). Hoboken, NJ: Wiley & Sons.

Federal Chief Information Officer. (2010). *25 point implementation plan to reform federal information technology management*. Retrieved from http://www.dhs.gov/sites/default/files/publications/digital-strategy/25-point-implementation-plan-to-reform-federal-it.pdf

Federal CIO Council. (2009). *2008 Clinger–Cohen core competencies*. Retrieved from http://www.cio.gov/Documents/2008%20Clinger-Cohen%20Core%20Competencies.pdf

Fortino, A. (2008). The new CIO: From technician to business strategist and the implications for e-commerce, e-business engineering. In *Proceedings of the IEEE International Conference on e-Business Engineering* (ICEBE '08) *(*pp. 139–146). doi: 10.1109/ICEBE.2008.67

Freeman, R. E. (2010). *Strategic management: A stakeholder approach*. Cambridge, UK: Cambridge University Press.

Glasow, P. (2005, April). *Fundamentals of survey research methodology*. Retrieved from http://www.mitre.org/work/tech_papers/tech_papers_05/05_0638/05_0638.pdf

Government Accountability Office (GAO). (2004). *Information technology investment management—A framework for assessing and improving process maturity* (GAO-04–394G). Washington, DC: Author. Retrieved from http://www.gao.gov/assets/80/76790.pdf

Government Accountability Office (GAO). (2007). *Business systems modernization: Strategy for evolving DoD's business enterprise architecture offers a conceptual approach, but execution details are needed: Report to congressional committees* (GAO-07–451). Washington, DC: Author. Retrieved from http://purl.access.gpo.gov/GPO/LPS82927

Government Accountability Office (GAO). (2011). *Information technology—Critical factors underlying successful major acquisitions* (GAO-12–7). Retrieved from http://www.gao.gov/assets/590/585842.pdf

Government Accountability Office (GAO). (2012). *Information security—Better implementation of controls for mobile devices should be encouraged* (GAO-12–757). Retrieved from http://www.gao.gov/assets/650/648519.pdf

Harris, S. (2010a). Access control. In J. Jue & R. Bart (Eds.), *CISSP all-in-one exam guide* 5th ed., pp. 153–279). New York, NY: McGraw-Hill.

Harris, S. (2010b). Botnets. In J. Jue & R. Bart (Eds.), *CISSP all-in-one exam guide* 5th ed., pp. 1020–1021). New York, NY: McGraw-Hill.

Hunter, M. G. (2011). Identifying issues of the chief information officer role through qualitative interviews. *International Journal of Sociotechnology and Knowledge Development (IJSKD), 3*(2), 42–52. doi:10.4018/jskd.2011040104

Jansen, W., Gavrilla, S., Séveillac, C., Heute, T., & Korolev, V. (2004). A unified framework for mobile device security. Paper presented at the International Conference on Security and Management. Retrieved from National Institute of Standards and Technology website: http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_devices/PP-UNIsecFramework-fin.pdf

Jansen, W., & Scarfone, K. (2008). *Guidelines on cell phone and PDA security recommendations of the National Institute of Standards and Technology* (NIST SP800–124). Retrieved from National Institute of Standards and Technology website: http://csrc.nist.gov/publications/nistpubs/800–124/SP800–124.pdf

Kaul, V., Makaya, C., Das, S., Shur, D., & Samtani, S. (2011, November). On the adaptation of commercial smartphones to tactical environments. In *Proceedings of the Military Communications Conference 2011 (MILCOM 2011)* (pp. 2205–2210). doi:10.1109/MILCOM.2011.6127649

Kelly, K. (2003). New rules for a new economy. *Wired Digital, Inc*. Retrieved from http://www.wired.com/wired/archive/5.09/newrules_pr.html

Kissel, R. (Ed.). (2012). *Glossary of key information security terms* (Vol. 2). Manuscript in preparation. Gaithersburg, MD: National Institute of Standards and Technology.

Lafranchise, P. A. (2012). Migrating Department of Defense (DoD) web service based applications to mobile computing platforms. Retrieved from http://hdl.handle.net/10945/6820

LaFrenier, K. J. (2011). Mobile security enclaves. Retrieved from http://hdl.handle.net/10945/5579

Liu, X., Madsen, C., & McDrew, D. (2002). *Cisco systems' simple certificate enrollment protocol (SCEP).* Manuscript submitted for publication.

Liu, L., Moulic, R., & Shea, D. (2010). Cloud service portal for mobile device management. In *Proceedings of the 2010 IEEE Seventh International Conference on E-Business Engineering* (pp. 474–478). doi:10.1109/ICEBE.2010.102

MaaS360. (2012). *Mobile device management glossary*. Retrieved from http://www.MaaS360.com

Microsoft. (2006, October). *Windows mobile device management and security solutions guide*. Retrieved from http://www.microsoft.com/windowsmobile

Miller, K. W., Voas, J., & Hurlburt, G. F. (2012, September/October). BYOD: Security considerations. *IT Pro*, 53–55.

The MITRE Corporation. (2012). *The National Security Engineering Center*. Retrieved from http://www.mitre.org/news/pdfs/nsec.pdf

Mont, M. C., & Brown, R. (2011). Risk assessment and decision support for security policies and related enterprise operational processes. In *Proceedings of the 2011 IEEE International Symposium on Policies for Distributed Systems and Networks* (pp. 137–140). doi:10.1109/POLICY.2011.19

Natchetoi, Y., Kaufman, V., & Shapiro, A. (2008). Service-oriented architecture for mobile applications. In *Proceedings of the 1st International Workshop on Software Architectures and Mobility* (pp. 27–32). Retrieved from http://dl.acm.org/citation.cfm?id=1370888.1370896

National Institute of Standards and Technology (NIST). (2012). *Security and privacy controls for federal information systems and organizations* (NIST SP 800–53 Rev. 4). Gaithersburg, MD: Author.

National Institute of Standards and Technology (NIST). (2013). Mobile security and forensics. Retrieved from http://www.nist.gov/itl/csd/ssa/mobile-security-forensics.cfm

National Security Agency (NSA) Central Security Service. (2013). Mission. Retrieved from http://www.nsa.gov/about/mission/index.shtml

Office of the Director of National Intelligence (ODNI). (2012, January 13). How intelligence works. Retrieved from http://www.intelligence.gov/about-the-intelligence-community/how-intelligence-works/data-gathering.html

Porter, G., Leader, P., Gordon, C. V., Karvonides, N., Kneece, R. R., & Neil, W. D. O. (2009, December). *The major causes of cost growth in defense acquisition: Volume II: Main body* (IDA Paper P-4531). Alexandria, VA: Institute for Defense Analyses.

Prohaska, B. (2011). Social media for the collaborative enterprise. *IT Professional Magazine, 13*(4), 61–63, 64.

Regard, D. L. (2012). Mobile devices: Catalyst for better records management? *Information Management Journal, 46*(5), 10–12.

Rhee, K., Jeon, W., & Won, D. (2012). Security requirements of a mobile device management system. *International Journal of Security and Its Applications*, *6*(2), 353–358. Retrieved from http://www.sersc.org/journals/IJSIA/vol6_no2_2012/49.pdf

Rose, C. (2012). Smart phone, dumb security. *Review of Business*, *16*(1), 21–26.

Ross, J. W., Weill, P., & Robertson, D. (2006a). *Enterprise architecture as strategy: Creating a foundation for business execution*. Boston, MA: Harvard Business School Press.

Ross, J. W., Weill, P., & Robertson, D. (2006b). *Enterprise architecture as strategy: Creating a foundation for business execution* [Presentation slide 1]. Retrieved from http://cisr.mit.edu/files/2009/12/Topic-EA_slide1_lg.png

Ross, J. W., Weill, P., & Robertson, D. (2006c). *Enterprise architecture as strategy: Creating a foundation for business execution* [Presentation slide 2]. Retrieved from http://cisr.mit.edu/files/2009/12/Topic-EA_slide2_lg.png

Ruebsamen, T., & Reich, C. (2012). Enhancing mobile device security by security level integration in a cloud proxy. In *Proceedings of Cloud Computing 2012, the Third International Conference on Cloud Computing, GRIDs and Virtualization* (pp. 159–168). Retrieved from http://www.thinkmind.org/index.php?view=article&articleid=cloud_computing_2012_7_30_20180

Scarfone, K., & Souppaya, M. (2012). *Guidelines for managing and securing mobile devices in the enterprise: Recommendations of the National Institute of Standards and Technology* (SP800–124 Rev. 1). Manuscript in preparation. Retrieved from National Institute of Standards and Technology website: http://csrc.nist.gov/publications/drafts/800–124r1/draft_sp800–124-rev1.pdf

Schuck, T. M. (2010). An extended enterprise architecture for a network-enabled, effects-based approach for national park protection. *Systems Engineering, 13*(3), 209–216.

Schultz, E. E., & Shpantzer, G. (2010). Information security management handbook. In H. F. Tipton & M. K. Nozaki (Eds.), *Security* (6th ed., pp. 107–125). Boca Raton, FL: CRC Press.

Shirazi, H. M. (2009). A framework for agile enterprise architecture. *International Journal of Intelligent Information Technology Application, 2*(4), 182–186.

Stalling, W., Brown, L., Bauer, M., & Howard, M. (2008a). Malicious software BOTS. In T. Dunkelberger & C. Snyder (Eds.), *Computer security: Principles and practice* (pp. 215–248). Upper Saddle River, NJ: Pearson Prentice Hall.

Stalling, W., Brown, L., Bauer, M., & Howard, M. (2008b). Man-in-the-middle attack. In T. Dunkelberger & C. Snyder (Eds.), *Computer security: Principles and practice* (pp. 625–649). Upper Saddle River, NJ: Pearson Prentice Hall.

Sue, V., & Ritter, L. (2012). *Conducting online surveys*. Thousand Oaks, CA: Sage.

Taiple, K. (2012, January 13). *Overview: What is cybercrime?* Retrieved from New York Law School—Cybercrime, Cyberterrorism, and Digital Law Enforcement website: http://www.information-retrieval.info/cybercrime/index01.html

The White House, Office of the Press Secretary. (2009, March 5). President Obama names Vivek Kundra chief information officer [Press release]. Retrieved from http://www.whitehouse.gov/the_press_office/President-Obama-Names-Vivek-Kundra-Chief-Information-Officer/

Toubiana, V. (2008). Towards a flexible security management solution for dynamic MANETs. In *Proceedings of the Network Operations and Management Symposium, 2008* (pp. 963–966). Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4575258

Viega, J., & Michael, B. (2010, March/April). Mobile device security. *IEEE Security & Privacy*, 11–12.

Walker, M. (2012a). Glossary. In T. Green (Ed.), *CEH certified ethical hacker exam guide* (pp. 339–371). New York, NY: McGraw-Hill.

Walker, M. (2012b). The security, functionality, and ease of use triangle. In T. Green (Ed.), *CEH certified ethical hacker exam guide* (pp. 1–25). New York, NY: McGraw Hill.

Whitehead, E. C., Sarkani, S., & Mazzuchi, T. A. (2011). Maximizing federal IT dollars: A connection between IT investments and organizational performance. *Defense AR Journal*, *18*(2), 176, 195.

Wilson, C. (2008). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for Congress* (CRS Report RL32114). Retrieved from http://www.fas.org/sgp/crs/terror/RL32114.pdf

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Glenn Cook
   Naval Postgraduate School
   Monterey, California

4. Brad Naegle
   Naval Postgraduate School
   Monterey, California

5. Douglas Brinkley
   Naval Postgraduate School
   Monterey, California

6. Dan Boger
   Naval Postgraduate School
   Monterey, California

7. William R. Gates
   Naval Postgraduate School
   Monterey, California